AFRL-OSR-VA-TR-2015-0164

Insertion, Detection, and Extraction of Messages

Dimitrios Pados
RESEARCH FOUNDATION OF STATE UNIVERSITY OF NEW YORK THE

07/09/2015
Final Report

Air Force Research Laboratory
AF Office Of Scientific Research (AFOSR)/ RTC
Arlington, Virginia 22203
Air Force Materiel Command

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*
14-07-2015

2. REPORT TYPE
Final Performance

3. DATES COVERED *(From - To)*
01-04-2012 to 31-03-2015

4. TITLE AND SUBTITLE
Insertion, Detection, and Extraction of Messages Hidden by Optimal Multi-Signature Spread Spectrum Means

5a. CONTRACT NUMBER

5b. GRANT NUMBER
FA9550-12-1-0123

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Dimitrios Pados

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
RESEARCH FOUNDATION OF STATE UNIVERSITY OF NEW YORK THE
402 CROFTS HALL
BUFFALO, NY 142600001 US

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
AF Office of Scientific Research
875 N. Randolph St. Room 3112
Arlington, VA 22203

10. SPONSOR/MONITOR'S ACRONYM(S)
AFOSR

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
A DISTRIBUTION UNLIMITED: PB Public Release

13. SUPPLEMENTARY NOTES

14. ABSTRACT

We carry out optimized spread-spectrum data embedding in a given digital image (or audio, or video sequence). First, the overall image/host medium is pre-processed into transform-domain small blocks from which host vectors are obtained via zig-zag scanning vectorization. Multiuser data embedding is performed in the generated host vectors. Under this data embedding model, we calculate an orthogonal set of embedding spread-spectrum signatures that achieves maximum sum signal-to-interference-plus-noise ratio (sum-SINR) at the output of the linearfilter receivers for any fixed embedding amplitude values. Then, for any given total embedding distortion constraint, we present the optimal multi-signature assignment and amplitude allocation that maximizes the sum capacity of the embedding procedure. The practical implication of the reported results is sum-SINR, sum-capacity optimal multiuser/multi-signature spread-spectrum data embedding in the digital medium. Extensive experiments that we carried out demonstrate the effectiveness of the proposed methods. The problem of extracting blindly data embedded over a wide band in a spectrum (transform) domain of a digital medium is also considered.

15. SUBJECT TERMS
spread-spectrum, data consealment, algorithmn

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Dimitrios Pados
U	U	U	UU		

					19b. TELEPHONE NUMBER *(Include area code)* 716-645-1150

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18

FINAL REPORT

Grant #: FA9550-12-1-0123

Project Title: Insertion, Detection, and Extraction of Messages Hidden by Optimal Multi-signature Spread-Spectrum Means

Reporting Period: April 1, 2012 - March 31, 2015

Prepared by: Dimitris A. Pados, Clifford C. Furnas Chair Professor and
Stella N. Batalama, Professor and Chair
Department of Electrical Engineering
The State University of New York at Buffalo
Buffalo, NY 14260

E-mail : {pados, batalama}@buffalo.edu

Contents

1 Abstract

In this work, we carry out optimized spread-spectrum concealment of multiuser data under a given digital image (or audio, or video sequence). First, the overall image/host medium is pre-processed into transform-domain small blocks from which host vectors are obtained via zig-zag scanning vectorization. Multiuser data hiding is performed in the generated host vectors. Under this data hiding system model, we calculate an orthogonal set of embedding spread-spectrum signatures that achieves maximum sum signal-to-interference-plus-noise ratio (sum-SINR) at the output of the linear-filter receivers for any fixed embedding amplitude values. Then, for any given total embedding distortion constraint, we present the optimal multi-signature assignment and amplitude allocation that maximizes the sum capacity of the concealment procedure. The practical implication of the reported results is sum-SINR, sum-capacity optimal multiuser/multi-signature spread-spectrum data hiding in the digital medium. Extensive experiments that we carried out demonstrate the effectiveness of the proposed methods.

We also consider the problem of extracting blindly data embedded over a wide band in a spectrum (transform) domain of a digital medium (image, audio, video). We develop a novel multi-carrier/signature iterative generalized least-squares (M-IGLS) core procedure to seek unknown data hidden in hosts via multi-carrier spread-spectrum embedding. Neither the original host nor the embedding carriers are assumed available. Experimental studies on images show that the developed algorithm can achieve recovery probability of error close to what may be attained with known embedding carriers and host autocorrelation matrix.

2 Introduction

Embedding digital data in digital host images has a broad range of applications, from annotation and single-stream media merging (text/audio/image) to watermarking and covert communications [1],[2] when embedding is to be carried out in a manner imperceptible by the human eye.

There are different approaches in the literature to embed digital data in a host image. Simple direct hiding in a given host is considered in [3]-[6]. Embedding information after full frame discrete fourier transform (DFT) or discrete cosine transform (DCT) image transformation is discussed in [7]-[10]. Concealing data after block DFT or DCT transformation of the host image is presented in [11],[12]. Concealing data after wavelet transformation of the original host image is described in [13],[14].

In this work, we consider the emerging concept of multiuser (multi-signature) data embedding where multiple messages are hidden with different embedding spread-spectrum signatures in the host image [15],[16]. The theoretical challenges of multiuser spread-spectrum data embedding in part parallel those problems encountered in the field of code-division multiple-access (CDMA) communications [17]. For CDMA signature design, in the theoretical context of complex/real-valued signature sets, the early work of Welch [18] on total-square-correlation (TSC) bounds was followed up by direct minimum-TSC designs [19],[20] and iterative distributed optimization algorithms [21],[22]. New bounds on the TSC of binary signature sets were found [23] that led to minimum-TSC optimal binary signature set designs for almost all signature lengths and set sizes [23]-[25]. The sum capacity, total asymptotic efficiency, and maximum squared correlation of the minimum-TSC binary sets were evaluated in [26]. New bounds and optimal designs for minimum TSC quaternary signature sets are derived in [27]. The problems of periodic and aperiodic TSC are treated in [28],[29]. Binary/quaternary adaptive signature design over multipath channels is discussed in [30],[31].

In this present work, based on the optimal orthogonal carriers that maximize the sum capacity of the multiple-access colored Gaussian vector channel presented in [32], we give the orthonormal set of signatures for multiuser spread-spectrum data hiding in digital images that offers maximum sum signal-to-interference-plus-noise ratio (sum-SINR) embedding in arbitrary transform domain images with any given embedding amplitude values. Moreover, for any given total host distortion budget we present a power (amplitude) allocation scheme that maximizes the Shannon sum-capacity of the multiuser data embedding system under the assumption of Gaussian distributed (transform-domain) host data. These theoretical findings establish optimality of the Gkizeli-Pados-Medley multisignature eigen-design algorithm [16] under the general requirement of an orthogonal multiuser signature set. Experimental studies and comparisons included herein illustrate the theoretical results.

The notation used in this report is as follows: $\{\cdot\}^T$ denotes the transpose operation; $\mathbb{R}^n$ denotes the n dimensional real field; $E\{\cdot\}$ represents statistical expectation; $\mathbf{I}_n$ is the identity matrix of size $n \times n$. We use boldface lowercase letters to denote column vectors and boldface uppercase letters to denote matrices.

3 System Model

Consider a host image $\mathbf{H} \in \mathscr{M}^{N_1 \times N_2}$, where $\mathscr{M}$ is the image pixel alphabet and $N_1 \times N_2$ is the image size in pixels. The overall host image $\mathbf{H}$ is partitioned into P small blocks. Each small block has $N_1 N_2/P$ pixels. Under the multiuser data embedding model introduced in [16], each small block $\mathbf{H}_1, \mathbf{H}_2, \ldots, \mathbf{H}_P$ is about to transport K hidden digital information bits, one for each different user potentially. We will perform data hiding in the real two-dimensional transform domain $\mathscr{T}$.

After transform calculation for each small block, the matrices of the transform-domain coefficients $\mathscr{T}(\mathbf{H}_p)$, $p = 1, 2, \ldots, P$, are vectorized by conventional "zig-zag scanning" to

$$\begin{aligned}\mathrm{Vec}\{\mathscr{T}(\mathbf{H}_p)\} \;=\;& [\mathscr{T}(\mathbf{H}_p)_{1,1} \;\; \mathscr{T}(\mathbf{H}_p)_{2,1} \;\; \mathscr{T}(\mathbf{H}_p)_{1,2} \\ & \mathscr{T}(\mathbf{H}_p)_{3,1} \;\; \mathscr{T}(\mathbf{H}_p)_{2,2} \;\; \mathscr{T}(\mathbf{H}_p)_{1,3} \;\; \ldots]^T \end{aligned} \tag{1}$$

where $\mathscr{T}(\mathbf{H}_p)_{i,j}$ denotes the (i,j)th element of matrix $\mathscr{T}(\mathbf{H}_p)$. Note that $\mathrm{Vec}\{\mathscr{T}(\mathbf{H}_p)\} \in \mathbb{R}^{N_1 N_2/P}$, $p = 1, 2, \cdots, P$.

The final host vectors

$$\mathbf{x}_p \in \mathbb{R}^L, \qquad p = 1, 2, \ldots, P, \tag{2}$$

of length $L \leq N_1 N_2/P$ are formed directly from any subset of coefficients of $\mathrm{Vec}\{\mathscr{T}(\mathbf{H}_p)\}$, $p = 1, 2, \cdots, P$. For example, we can have host vector length $L = N_1 N_2/P - 1$ by excluding only the dc coefficient $\mathscr{T}(\mathbf{H}_p)_{1,1}$, since modification of $\mathscr{T}(\mathbf{H}_p)_{1,1}$ is known to lead, in general, to visible image change in the pixel domain. We show the diagram of generating the host vectors from a given host image in Fig. 1.

The autocorrelation matrix of the transform-domain host vectors $\mathbf{x}$ is defined as

$$\mathbf{R}_x \triangleq E\left\{\mathbf{x}\mathbf{x}^T\right\} = \frac{1}{P}\sum_{p=1}^{P} \mathbf{x}_p \mathbf{x}_p^T \tag{3}$$

It is easy to verify that for general natural images $\mathbf{R}_x \neq \alpha \mathbf{I}_L$, $\alpha > 0$; that is, $\mathbf{R}_x$ is not constant-valued diagonal or "white" in field language. The host image example of Elaine is shown in Fig. 2 where $\mathscr{M}^{N_1 \times N_2} = \{0, 1, \cdots, 255\}^{256 \times 256}$. The image is partitioned into $P = \frac{256 \times 256}{8 \times 8} = 1024$ 8×8 small blocks. After two-dimensional DCT transformation of the small blocks and zig-zag scanning vectorization, we obtain $\mathrm{Vec}\{\mathscr{T}(\mathbf{H}_1)\}$, $\mathrm{Vec}\{\mathscr{T}(\mathbf{H}_2)\}$, $\cdots$, $\mathrm{Vec}\{\mathscr{T}(\mathbf{H}_{1024})\}$ with individual vector length 64. We exclude only the dc coefficients to form the final host vectors $\mathbf{x}_1,\ \mathbf{x}_2,\ \cdots,\ \mathbf{x}_{1024}$ of length $L = 63$. The host data autocorrelation matrix $\mathbf{R}_x$ is shown in Fig. 3. We can see that the host vectors can be considered/act as colored noise to data to be embedded.

Multiuser data hiding can carried out in the host vectors $\mathbf{x}_1,\ \mathbf{x}_2,\ \cdots,\ \mathbf{x}_P$. Assuming that there are K users of interest or signatures for spread-spectrum data embedding, the host vectors are modified to

$$\mathbf{y} = \sum_{i=1}^{K} A_i b_i \mathbf{s}_i + \mathbf{x} + \mathbf{n} \tag{4}$$

where $b_1, b_2, \ldots, b_K \in \{\pm 1\}$ are the individual message bits embedded simultaneously in $\mathbf{x} \in \{\mathbf{x}_1,\ \mathbf{x}_2,\ \cdots,\ \mathbf{x}_P\}$ with corresponding amplitudes $A_i > 0$ and normalized signatures $\mathbf{s}_i \in \mathbb{R}^L$, $\parallel \mathbf{s}_i \parallel = 1$, $i = 1, 2, \ldots, K$. The additive vector $\mathbf{n} \sim \mathscr{N}(\mathbf{0}, \sigma^2 \mathbf{I}_L)$ accounts in the model for possible external white Gaussian noise of variance σ^2. Embedded bits, host vectors $\mathbf{x}$, and noise vectors $\mathbf{n}$ are considered to be statistically independent from each other. The embedded bits themselves are considered as Bernoulli probability-1/2 random variables that are independent across time and users/messages.

For independent embedded bits (or orthogonal signatures), we can calculate the mean-square distortion over the original host image as

$$\mathscr{D} = E\left\{ \left\| \sum_{i=1}^{K} A_i b_i \mathbf{s}_i \right\|^2 \right\} = \sum_{i=1}^{K} A_i^2. \tag{5}$$

The distortion caused by each individual embedded message i, $i = 1, 2, \cdots, K$, is

$$\mathscr{D}_i = E\left\{ \left\| A_i b_i \mathbf{s}_i \right\|^2 \right\} = A_i^2. \tag{6}$$

Assume now that given $\mathbf{y}$, message $j \in \{1, 2, \ldots, K\}$ is the message of interest. With signal of interest $A_j b_j \mathbf{s}_j$ and respective total disturbance $\sum_{i=1 i\neq j}^{K} A_i b_i \mathbf{s}_i + \mathbf{x} + \mathbf{n}$ from (4), the linear filter that operates on $\mathbf{y}$ and offers maximum SINR at its output can be calculated using the Cauchy-Schwarz inequality [33] to be

$$\begin{aligned} \mathbf{w}_{maxSINR,j} &= \arg\max_{\mathbf{w}} \frac{E\left\{ \left| \mathbf{w}^T \left(A_j b_j \mathbf{s}_j \right) \right|^2 \right\}}{E\left\{ \left| \mathbf{w}^T \left(\sum_{i=1, i\neq j}^{K} A_i b_i \mathbf{s}_i + \mathbf{x} + \mathbf{n} \right) \right|^2 \right\}} \\ &= \mathbf{R}_{/j}^{-1} \mathbf{s}_j \end{aligned} \tag{7}$$

where matrix $\mathbf{R}_{/j}$ is defined as

$$\begin{aligned} \mathbf{R}_{/j} &\triangleq E\left\{ \left(\sum_{i=1, i\neq j}^{K} A_i b_i \mathbf{s}_i + \mathbf{x} + \mathbf{n} \right) \left(\sum_{i=1, i\neq j}^{K} A_i b_i \mathbf{s}_i + \mathbf{x} + \mathbf{n} \right)^T \right\} \\ &= \mathbf{R}_x + \sigma^2 \mathbf{I}_L + \sum_{i=1, i\neq j}^{K} A_i^2 \mathbf{s}_i \mathbf{s}_i^T. \end{aligned} \tag{8}$$

Note that $\mathbf{R}_{/j}$ is a function of $\mathbf{s}_1, \cdots, \mathbf{s}_{j-1}, \mathbf{s}_{j+1}, \cdots, \mathbf{s}_K$ and independent of $\mathbf{s}_j$.

Then, the output SINR value when we use the filter $\mathbf{w}_{maxSINR,j}$ can be calculated as

$$\begin{aligned} SINR_j &= A_j^2 \mathbf{s}_j^T \left(\mathbf{R}_x + \sigma^2 \mathbf{I}_L + \sum_{i=1, i\neq j}^{K} A_i^2 \mathbf{s}_i \mathbf{s}_i^T \right)^{-1} \mathbf{s}_j && (9) \\ &= A_j^2 \mathbf{s}_j^T \mathbf{R}_{/j}^{-1} \mathbf{s}_j. && (10) \end{aligned}$$

We define the metric of sum-SINR for the multiuser data embedding system as

$$sumSINR \triangleq \sum_{j=1}^{K} SINR_j. \tag{11}$$

As mentioned in [16], eq. (36), we can independently maximize $SINR_1$ for user 1 with respect to $\mathbf{s}_1$; then, maximize $SINR_2$ for user 2 with respect to $\mathbf{s}_2$, etc. After one optimization cycle over $\mathbf{s}_1$, $\mathbf{s}_2$, $\cdots, \mathbf{s}_K$, we can update $\mathbf{R}_{/1}, \mathbf{R}_{/2}, \cdots, \mathbf{R}_{/K}$ accordingly and run a second cycle over $\mathbf{s}_1, \mathbf{s}_2, \cdots, \mathbf{s}_K$. We may continue with optimization and update cycles until numerical convergence is observed. Regretfully, there is no known/guaranteed optimality of this described scheme. In this work, we will present a one-shot sum-SINR (and sum-capacity) optimal signature set assignment that operates directly on the transform-domain host data autocorrelation matrix $\mathbf{R}_x$ of (3).

4 Optimal Multisignature Embedding

First, we recall the Matrix Inversion Lemma [34] (also known as Woodbury's Identity),

$$(\mathbf{B} + \mathbf{UCV})^{-1} = \mathbf{B}^{-1} - \mathbf{B}^{-1}\mathbf{U}(\mathbf{C}^{-1} + \mathbf{VB}^{-1}\mathbf{U})^{-1}\mathbf{VB}^{-1}, \tag{12}$$

where $\mathbf{B}$, $\mathbf{U}$, $\mathbf{C}$ and $\mathbf{V}$ all denote matrices of appropriate size.

Then, we begin a tedious -yet all important- algebraic derivation of the $SINR$ expression for user j, $j = 1, 2, \cdots, K$, in (9). The application of the Matrix Inversion Lemma on equation (9) leads to

$$\begin{aligned} SINR_j &= A_j^2 \mathbf{s}_j^T \left(\mathbf{R}_x + \sigma^2 \mathbf{I}_L + \sum_{i=1, i\neq j}^{K} A_i^2 \mathbf{s}_i \mathbf{s}_i^T \right)^{-1} \mathbf{s}_j \\ &= \begin{cases} A_j^2 \mathbf{s}_j^T \left(\left(\mathbf{R}_x + \sigma^2 \mathbf{I}_L + \sum_{i=1, i\neq j}^{K-1} A_i^2 \mathbf{s}_i \mathbf{s}_i^T \right) + A_K^2 \mathbf{s}_K \mathbf{s}_K^T \right)^{-1} \mathbf{s}_j, & j \leq K-1, \\ A_j^2 \mathbf{s}_j^T \left(\left(\mathbf{R}_x + \sigma^2 \mathbf{I}_L + \sum_{i=1}^{K-2} A_i^2 \mathbf{s}_i \mathbf{s}_i^T \right) + A_{K-1}^2 \mathbf{s}_{K-1} \mathbf{s}_{K-1}^T \right)^{-1} \mathbf{s}_j, & j = K \end{cases} \\ &= SINR_j^{(K-1)} - T_j^{(K-1)}, && (13) \end{aligned}$$

where

$$SINR_j^{(K-1)} \triangleq \begin{cases} A_j^2 \mathbf{s}_j^T \left(\mathbf{R}_x + \sigma^2 \mathbf{I}_L + \sum_{i=1, i\neq j}^{K-1} A_i^2 \mathbf{s}_i \mathbf{s}_i^T \right)^{-1} \mathbf{s}_j, \\ \qquad\qquad j \leq K-1, \\ \\ A_j^2 \mathbf{s}_j^T \left(\mathbf{R}_x + \sigma^2 \mathbf{I}_L + \sum_{i=1}^{K-2} A_i^2 \mathbf{s}_i \mathbf{s}_i^T \right)^{-1} \mathbf{s}_j, \\ \qquad\qquad j = K, \end{cases} \tag{14}$$

$$T_j^{(K-1)} \triangleq \begin{cases} \frac{A_j^2 |\rho_j^{(K-1)}|^2}{1/A_K^2 + \mathbf{s}_K^T \left(\mathbf{R}_x + \sigma^2 \mathbf{I}_L + \sum_{i=1, i\neq j}^{K-1} A_i^2 \mathbf{s}_i \mathbf{s}_i^T \right)^{-1} \mathbf{s}_K}, \\ \qquad\qquad j \leq K-1, \\ \\ \frac{A_j^2 |\rho_j^{(K-1)}|^2}{1/A_{K-1}^2 + \mathbf{s}_{K-1}^T \left(\mathbf{R}_x + \sigma^2 \mathbf{I}_L + \sum_{i=1}^{K-2} A_i^2 \mathbf{s}_i \mathbf{s}_i^T \right)^{-1} \mathbf{s}_{K-1}}, \\ \qquad\qquad j = K, \end{cases} \tag{15}$$

and

$$\rho_j^{(K-1)} \triangleq \begin{cases} \mathbf{s}_j^T \left(\mathbf{R}_x + \sigma^2 \mathbf{I}_L + \sum_{i=1, i\neq j}^{K-1} A_i^2 \mathbf{s}_i \mathbf{s}_i^T \right)^{-1} \mathbf{s}_K, \\ \qquad\qquad j \leq K-1, \\ \\ \mathbf{s}_j^T \left(\mathbf{R}_x + \sigma^2 \mathbf{I}_L + \sum_{i=1}^{K-2} A_i^2 \mathbf{s}_i \mathbf{s}_i^T \right)^{-1} \mathbf{s}_{K-1}, \\ \qquad\qquad j = K. \end{cases} \tag{16}$$

Using again the Matrix Inversion Lemma on $SINR_j^{(K-1)}$ in (14), we obtain analogous expressions $SINR_j^{(K-2)}$, $T_j^{(K-2)}$, $\rho_j^{(K-2)}$. Continuing on repetitively, we obtain $SINR_j^{(K-3)}$, $T_j^{(K-3)}$, $\rho_j^{(K-3)}$,..., etc., of the general form $SINR_j^{(n)}$, $T_j^{(n)}$ and $\rho_j^{(n)}$, $1 \leq j \leq K$, $1 \leq n \leq K-1$, given below

$$SINR_j^{(n)} \triangleq \begin{cases} A_j^2 \mathbf{s}_j^T \left(\mathbf{R}_x + \sigma^2 \mathbf{I}_L + \sum_{i=1, i\neq j}^{n} A_i^2 \mathbf{s}_i \mathbf{s}_i^T \right)^{-1} \mathbf{s}_j, \\ \qquad\qquad j \leq n, \\ A_j^2 \mathbf{s}_j^T \left(\mathbf{R}_x + \sigma^2 \mathbf{I}_L + \sum_{i=1}^{n-1} A_i^2 \mathbf{s}_i \mathbf{s}_i^T \right)^{-1} \mathbf{s}_j, \\ \qquad\qquad j > n, \end{cases} \tag{17}$$

$$T_j^{(n)} \triangleq \begin{cases} \frac{A_j^2 |\rho_j^{(n)}|^2}{1/A_{n+1}^2 + \mathbf{s}_{n+1}^T \left(\mathbf{R}_x + \sigma^2 \mathbf{I}_L + \sum_{i=1, i\neq j}^{n} A_i^2 \mathbf{s}_i \mathbf{s}_i^T \right)^{-1} \mathbf{s}_{n+1}}, \\ \qquad\qquad j \leq n, \\ \\ \frac{A_j^2 |\rho_j^{(n)}|^2}{1/A_n^2 + \mathbf{s}_n^T \left(\mathbf{R}_x + \sigma^2 \mathbf{I}_L + \sum_{i=1}^{n-1} A_i^2 \mathbf{s}_i \mathbf{s}_i^T \right)^{-1} \mathbf{s}_n}, \\ \qquad\qquad j > n, \end{cases} \tag{18}$$

$$\rho_j^{(n)} \triangleq \begin{cases} \mathbf{s}_j^T \left(\mathbf{R}_x + \sigma^2 \mathbf{I}_L + \sum_{i=1, i\neq j}^{n} A_i^2 \mathbf{s}_i \mathbf{s}_i^T\right)^{-1} \mathbf{s}_{n+1}, \\ \qquad\qquad\qquad\qquad\qquad\qquad j \leq n, \\ \\ \mathbf{s}_j^T \left(\mathbf{R}_x + \sigma^2 \mathbf{I}_L + \sum_{i=1}^{n-1} A_i^2 \mathbf{s}_i \mathbf{s}_i^T\right)^{-1} \mathbf{s}_{n}, \\ \qquad\qquad\qquad\qquad\qquad\qquad j > n. \end{cases} \tag{19}$$

By (9), after $K-1$ application of the Matrix Inversion Lemma we reach

$$\begin{aligned} SINR_j &= SINR_j^{(K-1)} - T_j^{(K-1)} \\ &= SINR_j^{(K-2)} - T_j^{(K-2)} - T_j^{(K-1)} \\ &= \cdots \\ &= SINR_j^{(1)} - \sum_{n=1}^{K-1} T_j^{(n)}, \end{aligned} \tag{20}$$

where

$$SINR_j^{(1)} \triangleq A_j^2 \mathbf{s}_j^T \left(\mathbf{R}_x + \sigma^2 \mathbf{I}_L\right)^{-1} \mathbf{s}_j. \tag{21}$$

Accordingly, we can calculate the sum-SINR metric as

$$\begin{aligned} sumSINR &= \sum_{j=1}^{K} SINR_j \\ &= \sum_{j=1}^{K} SINR_j^{(1)} - \sum_{j=1}^{K} \sum_{n=1}^{K-1} T_j^{(n)}. \end{aligned} \tag{22}$$

Let $\{\mathbf{q}_1, \mathbf{q}_2, \ldots, \mathbf{q}_L\}$ be the L eigenvectors of $\mathbf{R}_x$ with corresponding eigenvalues $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_L$. The proof of the following Lemma comes directly from [32].

Lemma 1 *With orthonormal signature sets $\{\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_K\}$, $K \leq L$, for multiuser spread-spectrum data embedding and corresponding fixed embedding amplitudes $A_1 \geq A_2 \geq \ldots \geq A_K > 0$, $\sum_{j=1}^{K} SINR_j^{(1)}$ is maximized to $\sum_{j=1}^{K} \frac{A_j^2}{\lambda_{L-(j-1)}+\sigma^2}$ when $\mathbf{s}_1$, $\mathbf{s}_2$, $\ldots$, $\mathbf{s}_K$ are assigned as the K smallest-eigenvalue eigenvectors of the image host vectors autocorrelation matrix $\mathbf{R}_x$, i.e., $\mathbf{s}_j = \mathbf{q}_{L-(j-1)}$, $j = 1, 2, \ldots, K$. At the same time, when $\mathbf{s}_j = \mathbf{q}_{L-(j-1)}$, $j = 1, 2, \ldots, K$, $T_j^{(n)} = 0$ for every $j = 1, 2, \ldots, K$ and $n = 1, \ldots, K-1$.* □

Equipped with the result of Lemma 1 on equation (22), we return to the problem of optimal multiuser data embedding in host images by (4) and consider the multiuser performance metrics $sumSINR = \sum_{j=1}^{K} SINR_j$ and sum capacity C_{sum}, defined as the maximum information that can be obtained about the hidden variables $b_1, \ldots, b_K$ by examining the received vector $\mathbf{y}$ over all possible input probability distributions $f(b_1, \ldots, b_K)$,

$$C_{sum} \overset{\triangle}{=} \max_{f(b_1,\ldots,b_K)} \mathrm{I}(b_1, \ldots, b_K; \mathbf{y}). \tag{23}$$

If the transform-domain host data $\mathbf{x}$ can be assumed as Gaussian, the sum capacity of the data embedding scheme is [16]

$$C_{sum} = \frac{1}{2} \log_2 \det \left[\mathbf{I}_L + (\mathbf{R}_x + \sigma^2 \mathbf{I}_L)^{-1} \mathbf{S} \mathbf{A}^2 \mathbf{S}^T \right] \tag{24}$$

where $\mathbf{S} \overset{\triangle}{=} [\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_K]$ is the $L \times K$ matrix formed by the spread-spectrum embedding signatures and $\mathbf{A} \overset{\triangle}{=} \mathrm{diag}(A_1, A_2, \ldots, A_K)$ is the diagonal matrix of the embedding amplitudes.

The following theorem, built on Lemma 1, establishes the optimal orthonormal multiuser data embedding signature set for host images under fixed amplitude embedding.

Theorem 1 (Optimal Multi-signature Embedding)
For orthonormal signature sets $\{\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_K\}$, $K \leq L$, for multiuser spread-spectrum data embedding and corresponding fixed embedding amplitudes $A_1 \geq A_2 \geq \ldots \geq A_K > 0$, the sum-SINR is maximized to $sumSINR_{max} = \sum_{j=1}^{K} \frac{A_j^2}{\lambda_{L-(j-1)} + \sigma^2}$ when $\mathbf{s}_1$, $\mathbf{s}_2$, ..., $\mathbf{s}_K$ are assigned as the K smallest-eigenvalue eigenvectors of the image host vectors autocorrelation matrix $\mathbf{R}_x$, i.e., $\mathbf{s}_j = \mathbf{q}_{L-(j-1)}$, $j = 1, 2, \ldots, K$.
If the transform-domain host data $\mathbf{x}$ are Gaussian distributed, the same signature assignment maximizes sum capacity to $(C_{sum})_{max} = \frac{1}{2} \sum_{j=1}^{K} log_2 \left(1 + \frac{A_j^2}{\lambda_{L-(j-1)} + \sigma^2}\right)$ bits per K-symbol embedding. □

Hence, by Theorem 1, we proved that the sum-capacity optimality condition presented as necessary for multiuser spread-spectrum data hiding in Lemma 1 of [16] is also sufficient for general orthonormal signature set design. We can further consider individual embedding amplitudes as design parameters as well, within a total distortion budget. In other words, we can search for the optimal amplitude assignment that maximizes sum capacity for Gaussian host vectors subject to a total allowable distortion constraint $\mathscr{D} = \sum_{j=1}^{K} A_j^2$. The jointly optimal power allocation and signature assignment is presented in Theorem 2 below.

Theorem 2 (Optimal Multisignature Embedding and Power Allocation)
For orthonormal signature sets and a given total embedding distortion budget $\mathscr{D}$, the optimal (signature, amplitude) pairs that maximize the sum capacity for

multiuser data embedding in (transform-domain) Gaussian hosts are

$$\left(\mathbf{s}_j = \mathbf{q}_{L-(j-1)}, \quad A_j^2 = \left[-\left(\lambda_{L-(j-1)} + \sigma^2\right) + \mu\right]^+\right), \qquad j = 1, 2, \ldots, K,$$

where $[x]^+ \overset{\triangle}{=} max(x, 0)$ *and* μ *is the Kuhn-Tucker [35] coefficient chosen such that the distortion constraint* $\mathscr{D} = \sum_{j=1}^{K} A_j^2$ *is met with equality.* □

The amplitude/power allocation method described in Theorem 2 can be viewed as an eigen domain "waterfilling" procedure [35].

5 Experimental Studies on Embedding

In this section, we will first experiment on one image as an example and then show average results over the entire USC-SIPI database [36] of 44 miscellaneous images.

We first use as a host the familiar grayscale "Boat" image of size 512×512 in Fig. 4(a). We partition the image into small blocks of size 8×8 and calculate the DCT transform of each block. Then, we remove the dc coefficient from the zig-zag scanned DCT-domain vectors and create, this way, a host set of $512^2/8^2 = 4096$ vectors of length $L = 8 \times 8 - 1 = 63$. We hide $K = 15$ data messages via multiuser spread-spectrum embedding (15 bits in each block, each bit on a different signature) and include also additive white Gaussian noise of variance $\sigma^2 = 3dB$. Fig. 4(b) shows the Boat image after signature-set optimal multiuser spread-spectrum data hiding by Theorem 1 of this report at $\mathscr{D} = 20dB$ total distortion. The individual message amplitudes/distortions are fixed at $\mathscr{D}_1$, $\mathscr{D}_2 = \mathscr{D}_1 - 1dB$, $\cdots$, $\mathscr{D}_{15} = \mathscr{D}_{14} - 1dB$ ($1dB$ decrease for each successive message). Fig. 4(c) shows the Boat image after multiuser spread-spectrum data hiding at $\mathscr{D} = 20dB$ total distortion with jointly optimal signature set and amplitudes by Theorem 2 of this report. No perceptual difference can be observed by naked eye between the three images in Fig. 4.

In Fig. 5, we plot the sum-SINR of the messages reception process when the total embedding distortion $\mathscr{D}$ varies from 12 to 32dB and embedding is carried out with either (i) arbitrary or (ii) optimal signatures by Theorem 1. For this example, the gain in sum SINR by the use of the optimal signature set of Theorem 1 is at least $5dB$ and grows as the total allowed distortion increases. To translate sum-SINR to the more immediate and familiar metric of average bit-error-rate, in Fig. 6 we plot the corresponding average bit error rate (BER) of the recovered concealed messages. We can observe, for example, that when we use the optimal set of Theorem 1, to recover hidden messages with bit error rate 10^{-3} we need to cause only about $31dB$ distortion (including the accounted white noise). To have similar recovery error rate with arbitrary sequence-set embedding is not even practically possible per Fig. 6.

In Fig. 7, we examine the sum capacity of multiuser spread-spectrum data hiding under (i) arbitrary signature set design, (ii) signature optimization alone by Theorem 1, and (iii) optimal signature and power allocation by Theorem 2. At $32dB$ total distortion, an optimized signature set (with fixed per message distortion at $1dB$ increments) offers a gain of about 10 bits per embedding attempt over arbitrary signature sets. About 3 more bits are added when signature optimization is combined with optimal power allocation.

As a concluding evaluation effort, we carry out the experiments of Figs. 5 and 7 over the entire USC-SIPI database [36] of 44 miscellaneous images shown in Fig. 8 (16 color and 28 monochrome; 14 of size 256×256, 26 of size 512×512, and 4 of size 1024×1024.) Fig. 8 shows average sum SINR versus total distortion over the whole database. Fig. 9 shows average sum capacity results over the database. The average database findings of Figs. 9 and 10 are quite similar to the individual Boat results in Figs. 5 and 7 offering credible experimental support for the optimized multiuser embedding procedures described in this report.

6 Conclusions on Embedding

We considered the problem of multiuser spread-spectrum data hiding in transform-domain hosts (images in particular, herein) and identified the orthonormal signature set that offers maximum sum SINR embedding for any fixed embedding amplitude values. We showed that the set is also sum capacity optimal in terms of bits per multiuser embedding under the assumption that the transform-domain host data is Gaussian. When there is flexibility in assigning amplitudes across users under a total host distortion constraint, we derived the user amplitude values that not only meet the total constraint but also maximize sum capacity.

References

[1] F. Hartung and M. Kutter, "Multimedia watermarking techniques," *Proc. IEEE*, vol. 87, pp. 1079-1107, July 1999.

[2] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking digital image and video data: A state-of-the-art overview," *IEEE Signal Process. Mag.*, vol. 17, pp. 20-46, Sept. 2000.

[3] M. Kutter and S. Winkler, "A vision-based masking model for spread spectrum image watermarking," *IEEE Trans. Image Process.*, vol. 11, pp. 16-25, Jan. 2002.

[4] J. R. Smith and B. O. Comiskey, "Modulation and information hidding in images," *Lecture Notes Comput. Sci.*, vol. 1174, pp. 207-226, 1996.

[5] M. Wu and B. Liu, "Data hiding in binary image for authentication and annotation," *IEEE Trans. Multimedia.*, vol. 6, pp. 528-538, Aug. 2004.

[6] N. Nikolaidis and I. Pitas, "Robust image watermarking in the spatial domain," *Signal Process.*, vol. 66, pp. 385-403, May 1998.

[7] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shannon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Process.*, vol. 6, pp. 1673-1687, Dec. 1997.

[8] M. Barni, F. Bartolini, A. De Rosa, and A. Piva, "Optimum decoding and detection of multiplicative watermarks," *IEEE Trans. Signal Process.*, vol. 51, pp. 1118-1123, Apr. 2003.

[9] C. Qiang and T. S. Huang, "Robust optimum detection of transform domain multiplicative watermarks," *IEEE Trans. Signal Process.*, vol. 51, pp. 906-924, Apr. 2003.

[10] M. Barni, F. Bartolini, A. De Rosa, and A. Piva, "Capacity of full frame DCT image watermarks," *IEEE Trans. Image Process.*, vol. 9, pp. 1450-1455, Aug. 2000.

[11] J. Hernandez, M. Amado, and F. Perez-Gonzalez, "DCT-domain watermarking techniques for still images: Detector performance analysis and a new structure," *IEEE Trans. Image Process.*, vol. 9, pp. 55-68, Jan. 2000.

[12] C. B. Adsumilli, M. C. Q. Farias, S. K. Mitra, and M. Carli, "A robust error concealment technique using data hiding for image and video transmission over lossy channels," *IEEE Trans. Circuits Syst. Video Tech.*, vol. 15, pp. 1394-1406, Nov. 2005.

[13] P. Moulin and A. Ivanović, "The zero-rate spread-spectrum watermarking game," *IEEE Trans. Signal Process.*, vol. 51, pp. 1098-1117, Apr. 2003.

[14] X. G. Xia, C. G. Boncelet, and G. R. Arce, "A multiresolution watermark for digital images," in *Proc. IEEE Int. Conf. Image Process.*, Chicago, IL, Nov. 1998, vol. 1, pp. 548-551.

[15] M. Gkizeli, D. A. Pados, and M. J. Medley, "SINR, bit error rate, and Shannon capacity optimized spread-spectrum steganography," in *Proc. Int. Conf. Image Process.*, Singapore, Oct. 2004, vol. 3, pp. 1561-1564.

[16] M. Gkizeli, D. A. Pados, and M. J. Medley, "Optimal signature design for spread-spectrum steganography," *IEEE Trans. Image Process.*, vol. 16, pp. 391-405, Feb. 2007.

[17] S. Glisic and B. Vucetic, *Spread Spectrum CDMA Systems for Wireless Communications.* Norwood, MA: Artech House, 1997.

[18] L. R. Welch, "Lower bounds on the maximum cross correlation of signals," *IEEE Trans. Info. Theory*, vol. IT-20, pp. 397-399, May 1974.

[19] M. Rupf and J. L. Massey, "Optimum sequence multisets for synchronous code-division multiple-access channels," *IEEE Trans. Info. Theory*, vol. 40, pp. 1261-1266, July 1994.

[20] P. Viswanath, V. Anantharam, and D. N. C. Tse, "Optimal sequences, power control, and user capacity of synchronous CDMA systems with linear MMSE multiuser receivers," *IEEE Trans. Info. Theory*, vol. 45, pp. 1968-1983, Sept. 1999.

[21] C. Rose, S. Ulukus, and R. D. Yates, "Wireless systems and interference avoidance," *IEEE Trans. Wireless Commun.*, vol. 1, pp. 415-428, July 2002.

[22] P. Anigstein and V. Anantharam, "Ensuring convergence of the MMSE iteration for interference avoidance to the global optimum," *IEEE Trans. Info. Theory*, vol. 49, pp. 873-885, Apr. 2003.

[23] G. N. Karystinos and D. A. Pados, "New bounds on the total squared correlation and optimum design of DS-CDMA binary signature sets," *IEEE Trans. Commun.*, vol. 51, pp. 48-51, Jan. 2003.

[24] C. Ding, M. Golin, and T. Kløve, "Meeting the Welch and Karystinos-Pados bounds on DS-CDMA binary signature sets," *Designs, Codes and Cryptography*, vol. 30, pp. 73-84, Aug. 2003.

[25] V. P. Ipatov, "On the Karystinos-Pados bounds and optimal binary DS-CDMA signature ensembles," *IEEE Commun. Letters*, vol. 8, pp. 81-83, Feb. 2004.

[26] G. N. Karystinos and D. A. Pados, "The maximum squared correlation, total asymptotic efficiency, and sum capacity of minimum total-squared-correlation binary signature sets," *IEEE Trans. Inform. Theory*, vol. 51, pp. 348-355, Jan. 2005.

[27] M. Li, S. N. Batalama, D. A. Pados and J. D. Matyjas, "Minimum total-squared-correlatioin quaternary signature sets: new bounds and optimal designs," *IEEE Trans. Commun.*, vol. 57, no. 12, pp. 3662-3671, Dec. 2009.

[28] H. Ganapathy, D. A. Pados, and G. N. Karystinos, "New bounds and optimal binary signature sets Part I: Periodic total squared correlation," *IEEE Trans. Commun.*, vol. 59, pp. 1123-1132, Apr. 2011.

[29] H. Ganapathy, D. A. Pados, and G. N. Karystinos, "New bounds and optimal binary signature sets Part II: Aperiodic total squared correlation," *IEEE Trans. Commun.*, vol. 59, pp. 1411-1420, May 2011.

[30] L. Wei, S. N. Batalama, D. A. Pados and B. W. Suter, "Adaptive binary signature design for code-division multiplexing," *IEEE Trans. Wireless Commun.*, vol. 7, no. 7, pp. 2798-2804, July 2008.

[31] L. Wei and W. Chen, "Optimal binary/quaternary adaptive signature design for code-division multiplexing," *IEEE Trans. Wireless Commun.*, vol. 12, no. 2, pp. 840-849, Feb. 2013.

[32] L. Wei and D. A. Pados, "Optimal orthogonal carriers and sum-SINR/sum-capacity of the multiple-access vector channel," *IEEE Trans. Commun.*, vol. 60, no. 5, pp. 1188-1192, May 2012.

[33] D.G. Manolakis, V.K. Ingle, and S.M. Kogon, *Statistical and Adaptive Signal Processing.* New York: McGraw-Hill, 2000.

[34] C. D. Meyer, *Matrix Analysis and Applied Linear Algebra.* Philadelphia, PA: SIAM, 2000.

[35] T. M. Cover and J. A. Thomas, *Elements of Information Theory,* 2nd ed. New York: Wiley, 2006.

[36] *USC-SIPI Image Database*, [Online]. Available: http://http://sipi.usc.edu/database/database.php?volume=misc

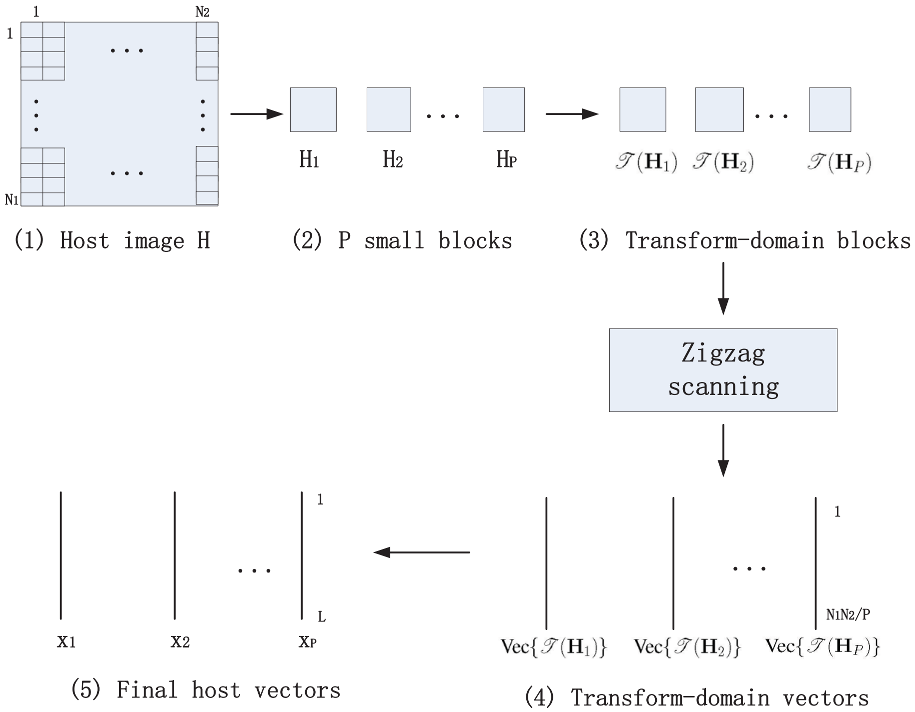

1
N2
1
N1
(1) Host image H
H1
H2
HP
(2) P small blocks
$\mathscr{T}(\mathbf{H}_1)$
$\mathscr{T}(\mathbf{H}_2)$
$\mathscr{T}(\mathbf{H}_P)$
(3) Transform-domain blocks
Zigzag scanning
1
N1N2/P
Vec{$\mathscr{T}(\mathbf{H}_1)$}
Vec{$\mathscr{T}(\mathbf{H}_2)$}
Vec{$\mathscr{T}(\mathbf{H}_P)$}
(4) Transform-domain vectors
1
L
x1
x2
xP
(5) Final host vectors

Figure 1: Host vectors generation diagram.

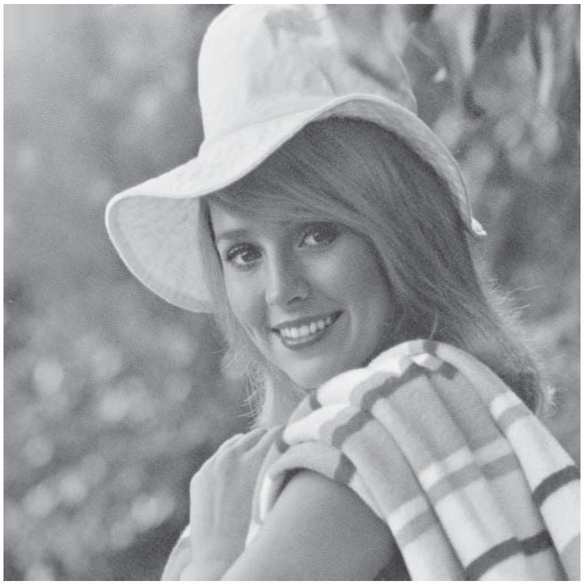


Figure 2: Host image example of Elaine.

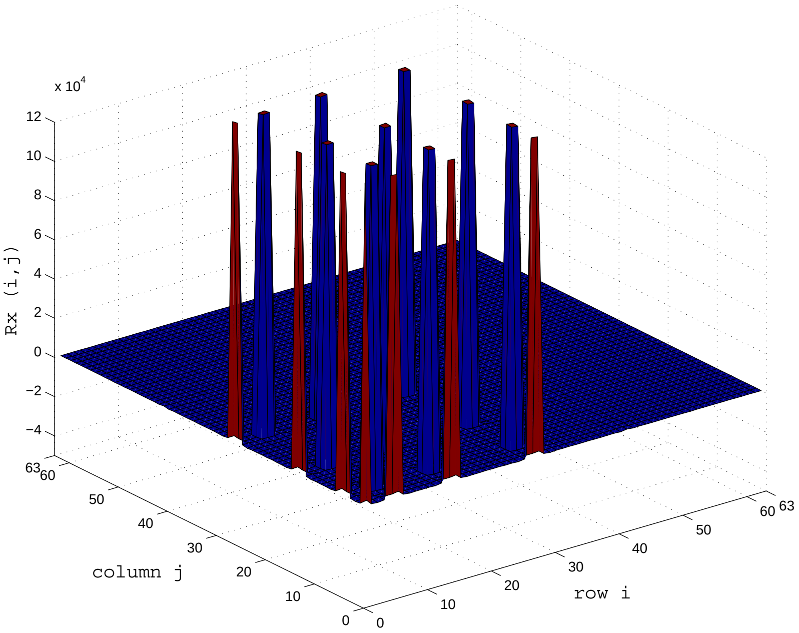
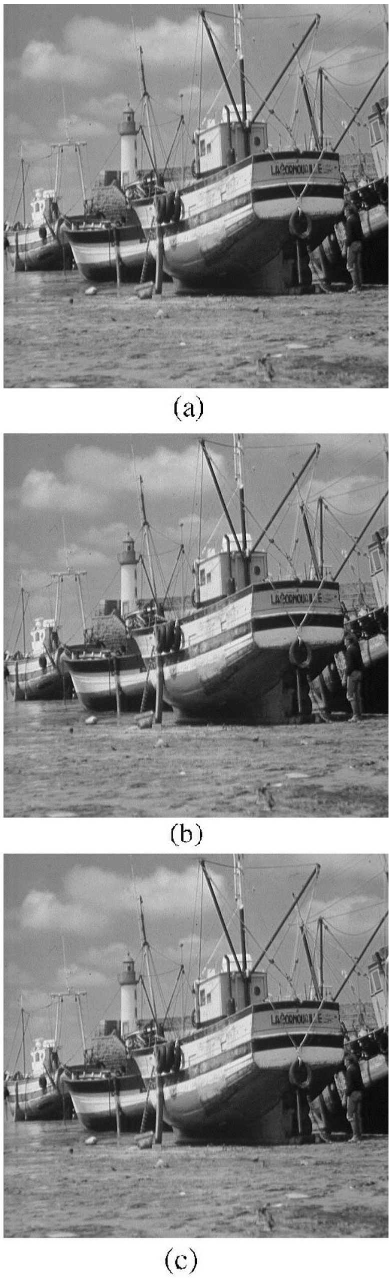


Figure 3: Host-vector autocorrelation matrix of Elaine.



(a)

(b)

(c)

Figure 4: (a) Original Boat image example (512×512 grayscale). (b) Boat image after optimal multi-signature embedding ($K = 15$ messages of size 4096 bits each, total distortion 20dB, fixed per message distortion $\mathscr{D}_{i+1} = \mathscr{D}_i - 1dB$, $i = 1, \cdots, K-1$, $\sigma_n^2 = 3dB$). (c) Boat image after optimal signature and power allocation ($K = 15$ messages of size 4096 bits each, total distortion 20dB, $\sigma_n^2 = 3dB$).

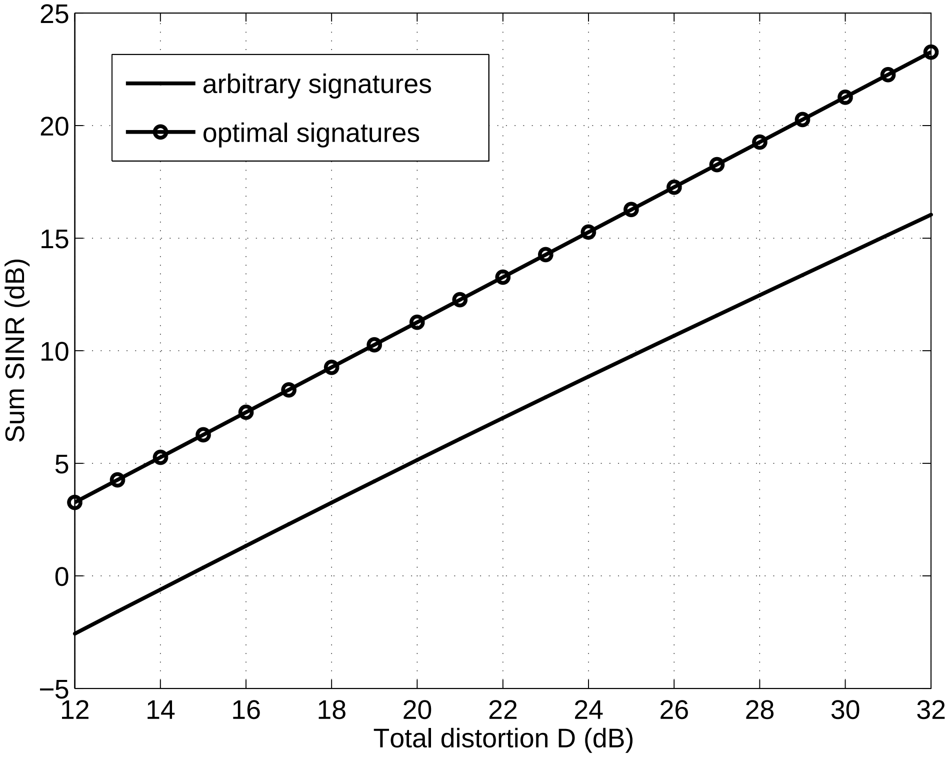


Figure 5: Sum SINR versus total distortion (Boat image, $K = 15$, $\mathscr{D}_{i+1} = \mathscr{D}_i - 1dB$, $i = 1, \cdots, K-1$, $\sigma^2 = 3dB$).

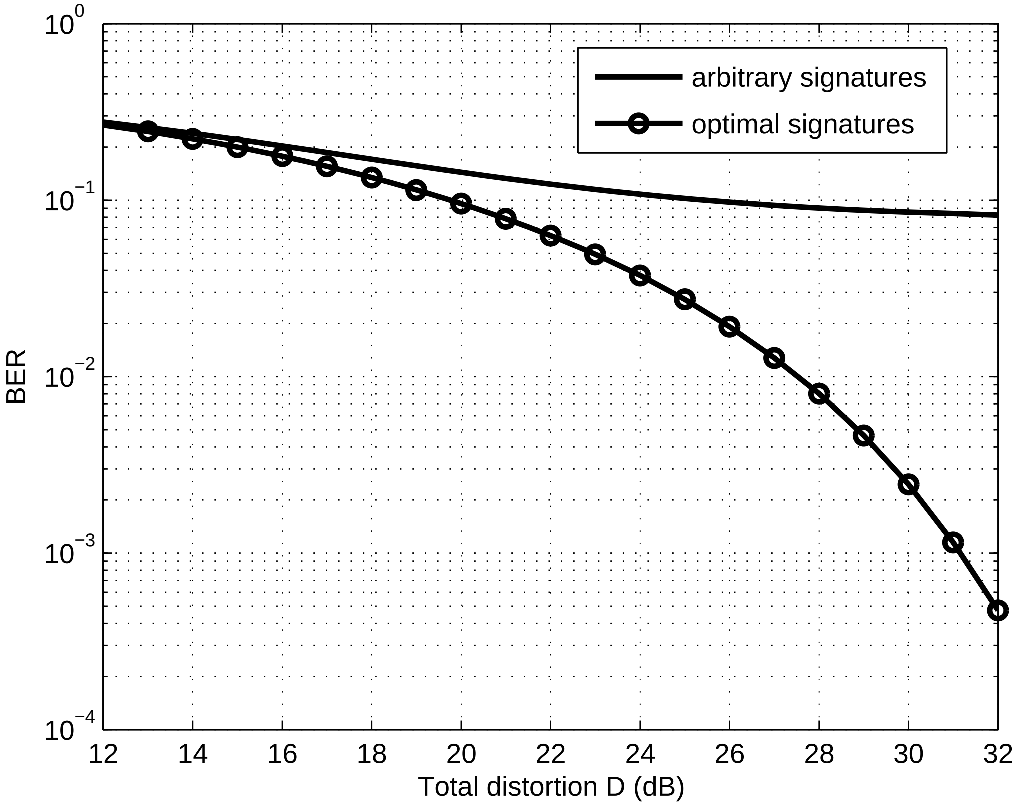


Figure 6: BER versus total distortion (Boat image, $K = 15$, $\mathscr{D}_{i+1} = \mathscr{D}_i - 1dB$, $i = 1, \cdots, K-1$, $\sigma^2 = 3dB$).

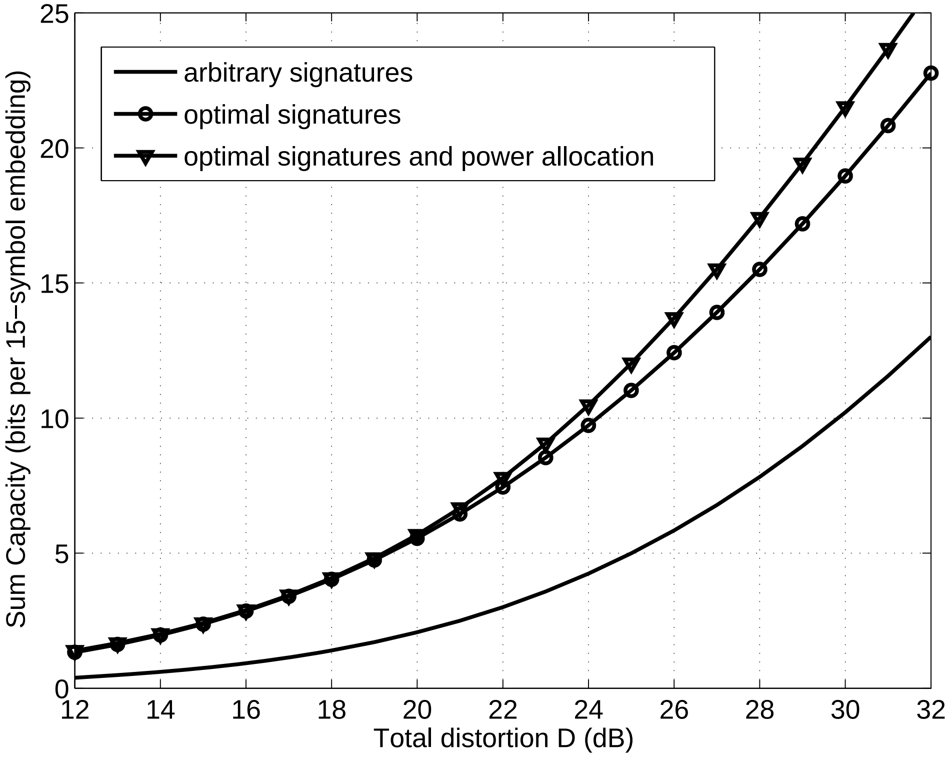


Figure 7: Sum capacity versus total distortion (Boat image, $K = 15$, $\sigma^2 = 3dB$).

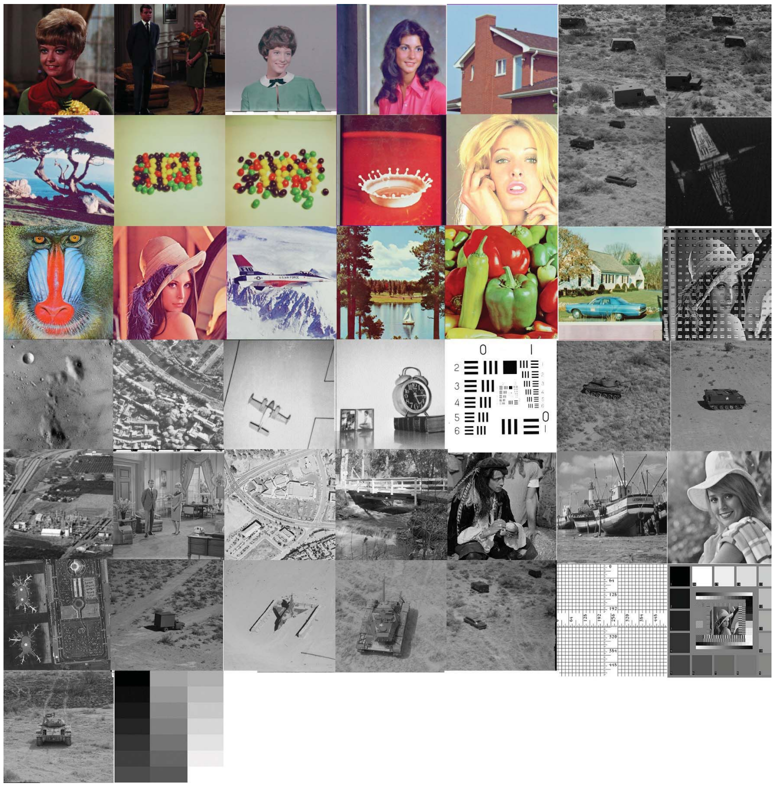


Figure 8: USC-SIPI image database of 44 images.

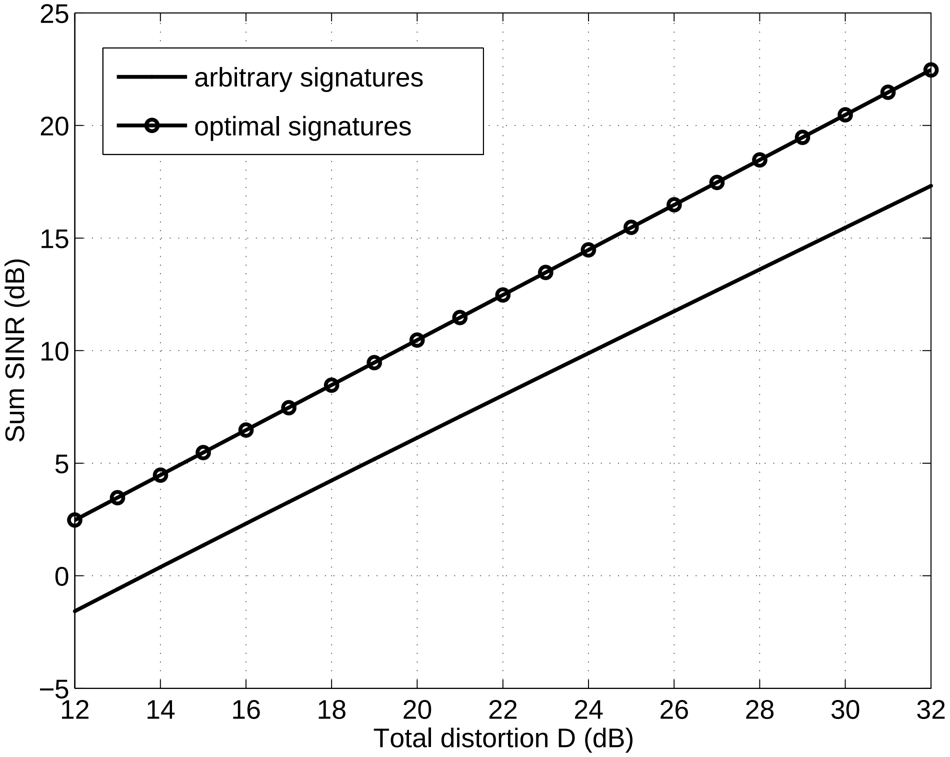


Figure 9: Sum SINR versus total distortion (average findings over USC-SIPI image database [36], $K = 15$, $\mathscr{D}_{i+1} = \mathscr{D}_i - 1dB$, $i = 1, \cdots, K-1$, $\sigma^2 = 3dB$).

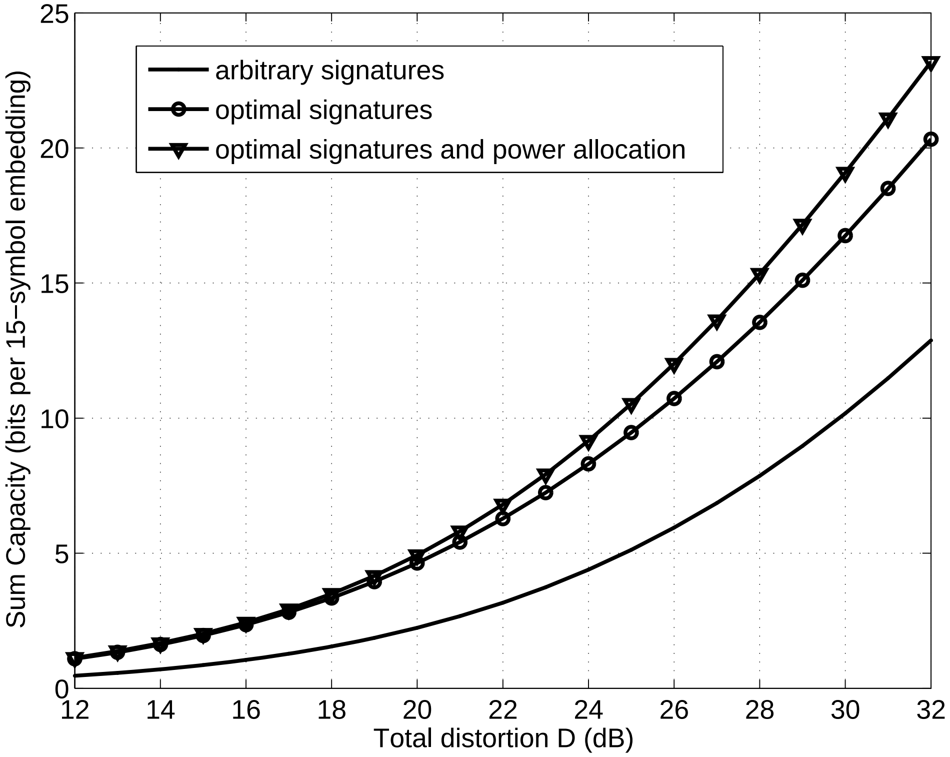


Figure 10: Sum capacity versus total distortion (average findings over USC-SIPI image database [36], $K = 15$, $\sigma^2 = 3dB$).

7 The Extraction Problem

Digital data embedding in digital media is an information technology field of rapidly growing commercial as well as national security interest. Applications may vary from annotation, copyright-marking, and watermarking, to single-stream media merging (text, audio, image) and covert communication [1]. In annotation, secondary data are embedded into digital multimedia to provide a way to deliver side information for various purposes; copyright-marking may act as permanent "iron branding" to show ownership; fragile watermarking may be intended to detect future tampering; hidden low-probability-to-detect (LPD) watermarking may serve as identification for confidential data validation or digital fingerprinting for tracing purposes [2]-[4]. Covert communication or steganography, which literally means "covered writing" in Greek, is the process of hiding data under a cover medium (also referred to as host), such as image, video, or audio, to establish secret communication between trusting parties and conceal the existence of embedded data [5]-[9]. As a general encompassing comment, different applications of information hiding, such as the ones identified above, require different satisfactory tradeoffs between the following four basic attributes of data hiding [10]: (*i*) Payload - information delivery rate; (*ii*) robustness - hidden data resistance to noise/disturbance; (*iii*) transparency - low host distortion for concealment purposes; and (*iv*) security - inability by unauthorized users to detect/access the communication channel.

Recently, developing data embedding technologies are being seen to pose a threat to personal privacy, commercial, and national security interests [11], [12]. In this work, we focus our attention on the blind recovery of secret data hidden in medium hosts via multi-carrier/signature direct-sequence spread-spectrum (DS-SS) transform domain embedding [13]-[20]. Neither the original host nor the embedding carriers (signatures or spreading sequences) are assumed known (fully blind data extraction). This blind hidden data extraction problem has also been referred to as "Watermarked content Only Attack" (WOA) in the watermarking security context [21]-[24].

While passive detection-only of the presence of embedded data is being intensively investigated in the past few years [25]-[33], active hidden data extraction is a relatively new branch of research. In blind extraction of SS embedded data, the unknown host acts as a source of interference/disturbance to the data to be recovered and, in a way, the problem parallels blind signal separation (BSS) applications as they arise in the fields of array processing, biomedical signal processing, and code-division multiple-access (CDMA) communication systems [34]-[38]. Under the assumption that the embedded secret messages are independent identically distributed (i.i.d.) random sequences and independent to the cover host, independent component analysis (ICA) may be utilized to pursue hidden data extraction [24], [39]. However, ICA-based BSS algorithms are not effective in the presence of correlated signal interference as is the case in SS multimedia embedding and degrade rapidly as the dimension of the carrier (signature) decreases relative to the message size. In [19], an iterative generalized least squares (IGLS) procedure was developed to blindly recover unknown messages hidden in image hosts via SS embedding. The algorithm has low complexity and strong recovery performance. However, the scheme is designed solely for *single-carrier* SS embedding where messages are hidden with one signature only and is not generalizable to the *multi-carrier* case. Realistically, an embedder would favor *multi-carrier* SS transform-domain embedding to increase security and/or payload rate.

In this work, we develop a novel multi-carrier iterative generalized least squares (M-IGLS) algorithm for SS hidden data extraction that, to the best of the authors' knowledge, appears for the first time in the broad communication theory and systems literature. For improved recovery performance, in particular for small hidden messages that pose the greatest challenge, experimental studies indicate that a few independent M-IGLS re-initializations and executions on the host can lead to hidden data recovery with probability of error close to what may be attained with known embedding carriers and known original host autocorrelation matrix. Applications of the developed algorithm are, of course, not limited to attacking steganographic covert communications by recovering the secret embedded messages. Since the carriers are also jointly estimated with the embedded data, the developed scheme can also be used for complete message removal or tampering attack as well by reinserting a fabricated message in place of the original. From the opposite data embedding point of view, the developed algorithm can be treated as a tool to test security robustness of SS data hiding schemes.

The following notation is used below. Boldface lower-case letters indicate column vectors and boldface upper-case letters indicate matrices; $\mathbb{R}$ denotes the set of all real numbers; $(\cdot)^T$ denotes matrix transpose; $\mathrm{Tr}\{\cdot\}$ is matrix trace; $\mathbf{I}_L$ is the $L \times L$ identity matrix; $\mathrm{sgn}\{\cdot\}$ denotes zero-threshold quantization; and $\mathbb{E}\{\cdot\}$ represents statistical expectation. Finally, $|\cdot|$, $\|\cdot\|$, and $\|\cdot\|_F$ are the scalar magnitude, vector norm, and matrix Frobenius norm, respectively.

8 Multi-carrier SS Embedding and Extraction: Problem Formulation

Consider a host image $\mathbf{H} \in \mathcal{M}^{N_1 \times N_2}$ where $\mathcal{M}$ is the finite image alphabet and $N_1 \times N_2$ is the image size in pixels. Without loss of generality, the image $\mathbf{H}$ is partitioned into M local non-overlapping blocks of size $\frac{N_1 N_2}{M}$. Each block, $\mathbf{H}_1, \mathbf{H}_2, ..., \mathbf{H}_M$, is to carry K hidden information bits (KM bits total image payload). Embedding is performed in a 2-D transform domain $\mathcal{T}$ (such as the discrete cosine transform, a wavelet transform, etc.). After transform calculation and vectorization (for example by conventional zig-zag scanning), we obtain $\mathcal{T}(\mathbf{H}_m) \in \mathbb{R}^{\frac{N_1 N_2}{M}}, m = 1, 2, \ldots, M$. From the transform domain vectors $\mathcal{T}(\mathbf{H}_m)$ we choose a fixed subset of $L \leq \frac{N_1 N_2}{M}$ coefficients (bins) to form the final host vectors $\mathbf{x}(m) \in \mathbb{R}^L$, $m = 1, 2, \ldots, M$. It is common and appropriate to avoid the dc coefficient (if applicable) due to high perceptual sensitivity in changes of the dc value.

The autocorrelation matrix of the host data $\mathbf{x}$ is an important statistical quantity for our developments and is defined as $\mathbf{R}_{\mathrm{x}} \triangleq \mathbb{E}\{\mathbf{x}\mathbf{x}^T\} = \frac{1}{M}\sum_{m=1}^{M}\mathbf{x}(m)\mathbf{x}(m)^T$. It is easy to verify that in general $\mathbf{R}_{\mathrm{x}} \neq \alpha\mathbf{I}_L, \alpha > 0$; that is, $\mathbf{R}_{\mathrm{x}}$ is *not* constant-value diagonal or "white" in field language. For example, 8×8 DCT with 63-bin host data formation (excluding only the dc coefficient) for the 256×256 gray-scale Baboon image in Fig. 11(a) gives the host autocorrelation matrix $\mathbf{R}_{\mathrm{x}}$ in Fig. 11(b) [20].

8.1 Multi-carrier SS Embedding

We consider K distinct message bit sequences, $\{b_k(1), b_k(2), \ldots, b_k(M)\}$, $k = 1, 2, \ldots, K$, $b_k(m) \in \{\pm 1\}$, $m = 1, \ldots, M$, each of length M bits. The K message sequences may be to be delivered to K distinct corresponding recipients or they are just K portions of one large message sequence to be transmitted to one recipient. In particular, the mth bit from each of the K sequences, $b_1(m), \ldots, b_K(m)$, is simultaneously hidden in the mth transform-domain host vector $\mathbf{x}(m)$ via additive SS embedding by means of K spreading sequences (carriers) $\mathbf{s}_k \in \mathbb{R}^L$, $\|\mathbf{s}_k\| = 1$, $k = 1, 2, \ldots, K$,

$$\mathbf{y}(m) = \sum_{k=1}^{K} A_k b_k(m)\mathbf{s}_k + \mathbf{x}(m) + \mathbf{n}(m),\ m = 1, 2, \ldots, M, \tag{25}$$

with corresponding amplitudes $A_k > 0$, $k = 1, \ldots, K$. For the sake of generality, $\mathbf{n}(m)$ represents potential external white Gaussian noise[1] of mean $\mathbf{0}$ and autocorrelation matrix $\sigma_n^2\mathbf{I}_L$, $\sigma_n^2 > 0$. It is assumed that $b_k(m)$ behave as equi-probable binary random variables that are independent in m (message bit sequence) and k (across messages). The contribution of each individual embedded message bit b_k to the composite signal is $A_k b_k \mathbf{s}_k$ and the block mean-squared distortion to the original host data $\mathbf{x}$ due to the embedded k message alone is

$$\mathcal{D}_k = \mathbb{E}\{\|A_k\mathbf{s}_k b_k\|^2\} = A_k^2,\ \ k = 1, 2, ..., K. \tag{26}$$

Under statistical independence of messages, the block mean-squared distortion of the original image due to the total, multi-message, insertion of data is $\mathcal{D} = \sum_{k=1}^{K} A_k^2$.

The intended recipient of the kth message with knowledge of the kth carrier $\mathbf{s}_k$ can perform embedded bit recovery by looking at the sign of the output of the minimum-mean-square-error (MMSE) filter $\mathbf{w}_{MMSE,k} = \mathbf{R}_{\mathrm{y}}^{-1}\mathbf{s}_k$,

$$\hat{b}_k(m) = \mathrm{sgn}\{\mathbf{w}_{MMSE,k}^T\mathbf{y}(m)\} = \mathrm{sgn}\{\mathbf{s}_k^T\mathbf{R}_{\mathrm{y}}^{-1}\mathbf{y}(m)\} \tag{27}$$

where $\mathbf{R}_{\mathrm{y}}$ is the autocorrelation matrix of the host-plus-data-plus-noise vectors

$$\mathbf{R}_{\mathrm{y}} \triangleq \mathbb{E}\{\mathbf{y}\mathbf{y}^T\} = \mathbf{R}_{\mathrm{x}} + \sum_{k=1}^{K} A_k^2\mathbf{s}_k\mathbf{s}_k^T + \sigma_n^2\mathbf{I}_L. \tag{28}$$

[1] Additive white Gaussian noise is frequently viewed as a suitable (most entropic) model for general quantization errors, channel transmission disturbances, and/or image processing attacks [40].

The autocorrelation matrix $\mathbf{R}_{\mathrm{y}}$ can be estimated by sample averaging over the set of M received vectors $\{\mathbf{y}(m)\}_{m=1}^{M}$, $\widehat{\mathbf{R}}_{\mathrm{y}} = \frac{1}{M}\sum_{m=1}^{M}\mathbf{y}(m)\mathbf{y}(m)^{T}$. Using $\widehat{\mathbf{R}}_{\mathrm{y}}$ in (27) in place of $\mathbf{R}_{\mathrm{y}}$, we obtain what is known as the sample-matrix-inversion MMSE (SMI-MMSE) detector implementation [34].

8.2 Formulation of the Extraction Problem

To blindly extract spread-spectrum embedded data from a given host image, the analyst needs first to convert the host to observation vectors of the form of $\mathbf{y}(m)$, $m = 1, \ldots, M$, in (25). This requires knowledge of (*i*) the partition, (*ii*) transform domain, (*iii*) subset of coefficients, and (*iv*) number of carriers used by the embedder. The host image partition (and block size N_1N_2/M in our notation) may be estimated by neighboring-pixels difference techniques as in [30]. Regarding the subset of coefficients used in embedding, the conservative approach is to assume that all coefficients are used, except maybe the dc value, and set accordingly $L = N_1N_2/M - 1$. The number of carriers K can be estimated by SS signal population identification algorithms such as in [41]. Finally, determination of the transform domain used in embedding seems to be a hurdle not yet tackled by current research. The natural approach would be to consider individually and exhaustively one transform at a time starting from the most common (for example, 2D-DCT, common wavelet transforms, and so on).

In this report, we focus the technical presentation solely after the point that the analyst obtains transform-domain observations in the form of $\mathbf{y}(m)$ in (25), upon performing appropriate image partition and transform calculation. We denote the combined "disturbance" to the hidden data (host plus noise) by $\mathbf{z}(m) \triangleq \mathbf{x}(m) + \mathbf{n}(m)$ and rewrite SS embedding by (25) as

$$\mathbf{y}(m) = \sum_{k=1}^{K} A_k b_k(m)\mathbf{s}_k + \mathbf{z}(m),\ m = 1, \ldots, M, \tag{29}$$

where $\mathbf{z}(m)$ is modeled as a sequence of zero-mean (without loss of generality) vectors with autocovariance matrix $\mathbf{R}_{\mathrm{z}} = \mathbb{E}\{\mathbf{z}\mathbf{z}^{T}\} = \mathbf{R}_{\mathrm{x}} + \sigma_n^2\mathbf{I}$. Let $\mathbf{v}_k \triangleq A_k\mathbf{s}_k \in \mathbb{R}^{L}$, $k = 1, \ldots, K$, be the amplitude-including embedding carriers. Then, we can further reformulate SS embedding as

$$\begin{aligned} \mathbf{y}(m) &= \sum_{k=1}^{K} b_k(m)\mathbf{v}_k + \mathbf{z}(m) && (30) \\ &= \mathbf{V}\mathbf{b}(m) + \mathbf{z}(m),\ m = 1, \ldots, M, && (31) \end{aligned}$$

where $\mathbf{V} \triangleq [\mathbf{v}_1, \ldots, \mathbf{v}_K] \in \mathbb{R}^{L\times K}$ is the amplitude-including carrier matrix and $\mathbf{b}(m) \in \{\pm 1\}^{K\times 1}$ is the vector of bits embedded in the mth host block. For notational simplicity, we can write the whole observation data in the form of one matrix

$$\mathbf{Y} = \mathbf{V}\mathbf{B} + \mathbf{Z} \tag{32}$$

where $\mathbf{Y} \triangleq [\mathbf{y}(1)\, \mathbf{y}(2) \dots \mathbf{y}(M)] \in \mathbb{R}^{L\times M}$, $\mathbf{B} \triangleq [\mathbf{b}(1)\, \mathbf{b}(2) \dots \mathbf{b}(M)] \in \{\pm 1\}^{K\times M}$, and $\mathbf{Z} \triangleq [\mathbf{z}(1)\, \mathbf{z}(2) \dots \mathbf{z}(M)] \in \mathbb{R}^{L\times M}$.

Our objective is to blindly extract the unknown hidden data $\mathbf{B}$ from the observation matrix $\mathbf{Y}$ without prior knowledge of the embedding carriers $\mathbf{s}_k$ and amplitudes A_k, $k = 1, \dots, K$, in $\mathbf{V} = [A_1\mathbf{s}_1, \dots, A_K\mathbf{s}_K]$ or the host medium itself $\mathbf{x}(1), \dots, \mathbf{x}(M)$ in $\mathbf{Z} = [\mathbf{x}(1) + \mathbf{n}(1), \dots, \mathbf{x}(M) + \mathbf{n}(M)]$.

9 Hidden Data Extraction

If $\mathbf{Z}$ were to be modeled as Gaussian distributed, the joint maximum-likelihood (ML) estimator of $\mathbf{V}$ and decoder of $\mathbf{B}$ would be

$$\widehat{\mathbf{V}}, \widehat{\mathbf{B}} = \arg \min_{\substack{\mathbf{B}\in\{\pm1\}^{(K\times M)},\\ \mathbf{V}\in\mathbb{R}^{L\times K}}} \|\mathbf{R}_{\mathrm{z}}^{-\frac{1}{2}}(\mathbf{Y} - \mathbf{V}\mathbf{B})\|_F^2 \tag{33}$$

where multiplication by $\mathbf{R}_{\mathrm{z}}^{-\frac{1}{2}}$ can be interpreted as prewhitening of the compound observation data. If Gaussianity of $\mathbf{Z}$ is not to be invoked, then (33) can be simply referred to as the joint generalized least-squares (GLS) solution[2] of $\mathbf{V}$ and $\mathbf{B}$.

The global GLS-optimal message matrix $\widehat{\mathbf{B}}$ in (33) can be computed independently of $\widehat{\mathbf{V}}$ by exhaustive search over all possible choices under the criterion function $\|\mathbf{R}_{\mathrm{z}}^{-\frac{1}{2}}\mathbf{Y}\mathbf{P}_{\perp\mathbf{B}}\|_F^2$,

$$\widehat{\mathbf{B}} = \arg \min_{\mathbf{B}\in\{\pm1\}^{K\times M}} \|\mathbf{R}_{\mathrm{z}}^{-\frac{1}{2}}\mathbf{Y}\mathbf{P}_{\perp\mathbf{B}}\|_F^2 \tag{34}$$

where $\mathbf{P}_{\perp\mathbf{B}} \triangleq \mathbf{I} - \mathbf{B}^T(\mathbf{B}\mathbf{B}^T)^{-1}\mathbf{B}$. The derivation of (34) is provided in the Appendix. Exhaustive search has, of course, complexity exponential in KM (total size of hidden messages in bits). We consider this cost unacceptable and attempt to reach a quality approximation of the solution of (34) (or (33), to that respect) by alternating generalized least-squares estimates of $\mathbf{V}$ and $\mathbf{B}$, iteratively, as described below.

Pretend $\mathbf{B}$ is known. The generalized least-squares estimate of $\mathbf{V}$ is

$$\begin{aligned} \widehat{\mathbf{V}}_{\mathrm{GLS}} &= \arg \min_{\mathbf{V}\in\mathbb{R}^{L\times K}} \|\mathbf{R}_{\mathrm{z}}^{-\frac{1}{2}}(\mathbf{Y} - \mathbf{V}\mathbf{B})\|_F^2 \\ &= \mathbf{Y}\mathbf{B}^T(\mathbf{B}\mathbf{B}^T)^{-1}. \end{aligned} \tag{35}$$

Pretend, in turn, that $\mathbf{V}$ is known. Then, the least-squares estimate of $\mathbf{B}$ *over the real field* is

$$\begin{aligned} \widehat{\mathbf{B}}_{\mathrm{GLS}}^{\mathrm{real}} &= \arg \min_{\mathbf{B}\in\mathbb{R}^{K\times M}} \|\mathbf{R}_{\mathrm{z}}^{-\frac{1}{2}}(\mathbf{Y} - \mathbf{V}\mathbf{B})\|_F^2 \\ &= (\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V})^{-1}\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{Y}. \end{aligned} \tag{36}$$

[2] Generalized least-squares solutions are weighted least-squares (WLS) solutions with optimal weighting matrices, here $\mathbf{R}_{\mathrm{z}}^{-\frac{1}{2}}$, that yield the lowest variance of the estimation error [35],[36].

Observing that

$$(\mathbf{V}^T\mathbf{R}_{\rm z}^{-1}\mathbf{V})^{-1}\mathbf{V}^T\mathbf{R}_{\rm z}^{-1} = (\mathbf{V}^T\mathbf{R}_{\rm y}^{-1}\mathbf{V})^{-1}\mathbf{V}^T\mathbf{R}_{\rm y}^{-1}, \tag{37}$$

we rewrite

$$\widehat{\mathbf{B}}_{\rm GLS}^{\rm real} = (\mathbf{V}^T\mathbf{R}_{\rm y}^{-1}\mathbf{V})^{-1}\mathbf{V}^T\mathbf{R}_{\rm y}^{-1}\mathbf{Y} \tag{38}$$

and suggest the approximate binary message solution

$$\begin{aligned}\widehat{\mathbf{B}}_{\rm GLS}^{\rm binary} &= \arg\min_{\mathbf{B}\in\{\pm1\}^{K\times M}} \|\mathbf{R}_{\rm z}^{-\frac{1}{2}}(\mathbf{Y}-\mathbf{V}\mathbf{B})\|_F^2 \\ &\simeq \operatorname{sgn}\{(\mathbf{V}^T\mathbf{R}_{\rm y}^{-1}\mathbf{V})^{-1}\mathbf{V}^T\mathbf{R}_{\rm y}^{-1}\mathbf{Y}\}.\end{aligned} \tag{39}$$

The proofs of (35), (36), and (37) are provided in the Appendix.

The *multi-carrier iterative generalized least-squares* (M-IGLS) procedure suggested by the two equations (35) and (39) is now straightforward. Initialize $\widehat{\mathbf{B}}$ arbitrarily and alternate iteratively between (35) and (39) to obtain at each step conditionally generalized least squares estimates of one matrix parameter given the other. Stop when convergence is observed. Notice that (39) utilizes knowledge of the autocorrelation matrix $\mathbf{R}_{\rm y}$, which can be estimated by sample averaging over the received data observations, $\widehat{\mathbf{R}}_{\rm y} = \frac{1}{M}\sum_{m=1}^{M}\mathbf{y}(m)\mathbf{y}(m)^T$. The M-IGLS extraction algorithm is summarized in Table 1. Superscripts denote iteration index. The computational complexity of each iteration of the M-IGLS algorithm is $\mathcal{O}(2K^3 + 2LMK + K^2(3L+M) + L^2K)$ and, experimentally, the number of iterations executed is between 20 and 50 in general.

For the sake of mathematical accuracy, we recall that in least-squares there is always a symbol sign (phase in complex domains) ambiguity when joint data extraction and carrier estimation is pursued (i.e., data bits $\mathbf{b}_k \in \{\pm1\}^M$ on carrier $\mathbf{s}_k \in \mathbb{R}^L$ have the same least-squares error with data bits $-\mathbf{b}_k$ on carrier $-\mathbf{s}_k$, $k = 1,\ldots,K$). The sign-ambiguity problem can be overcome with a few known or guessed data symbols for supervised sign correction[3] [42]. Moreover, in a multi-carrier least-squares scenario as the one that we face herein, the index association remains unresolved (i.e., given a recovered (message, carrier) pair ($\mathbf{b}$, $\mathbf{s}$), the corresponding index $k \in \{1,\ldots,K\}$ in (25) cannot be obtained). To the extend that the application of the work presented in this report is to simply extract blindly the embedded bits with the least possible errors, the carrier indexing problem is not dealt with any further.

Returning to the proposed data extraction algorithm, we understand that with arbitrary initialization convergence of the M-IGLS procedure described in Table 1 to the optimal GLS solution of (33) is not guaranteed in general. Extensive experimentation with the algorithm in Table 1 indicates that, for sufficiently long messages hidden by each carrier (M = 4Kbits or more, for example), satisfactory quality message decisions $\widehat{\mathbf{B}}$ can be directly obtained. However, when

[3] If the embedded data are encrypted, then both options $\mathbf{b}_k$ and $-\mathbf{b}_k$ must be separately decrypted and investigated for sign correction for each message $k = 1,\ldots,K$.

Table 1: Multi-carrier Iterative generalized least-squares Data Extraction

```
1) $d := 0$; initialize $\widehat{\mathbf{B}}^{(0)} \in \{\pm 1\}^{K \times M}$ arbitrarily.
2) $d := d + 1$;
   $\widehat{\mathbf{V}}^{(d)} := \mathbf{Y}(\widehat{\mathbf{B}}^{(d-1)})^T \left[(\widehat{\mathbf{B}}^{(d-1)})(\widehat{\mathbf{B}}^{(d-1)})^T\right]^{-1}$;
   $\widehat{\mathbf{B}}^{(d)} := \operatorname{sgn}\left\{\left((\widehat{\mathbf{V}}^{(d)})^T \widehat{\mathbf{R}}_{\mathrm{y}}^{-1} (\widehat{\mathbf{V}}^{(d)})\right)^{-1} (\widehat{\mathbf{V}}^{(d)})^T \widehat{\mathbf{R}}_{\mathrm{y}}^{-1} \mathbf{Y}\right\}$.
3) Repeat Step 2 until $\widehat{\mathbf{B}}^{(d)} = \widehat{\mathbf{B}}^{(d-1)}$.
```

the message size is small, M-IGLS may very well converge to inappropriate points/solutions. The quality (generalized-least-squares fit) of the end convergence point depends heavily on the initialization point and arbitrary initialization -which at first sight is unavoidable for blind data extraction- offers little assurance that the iterative scheme will lead us to appropriate, "reliable" (close to minimal generalized least-squares fit) solutions. To that respect, re-initialization and re-execution of the M-IGLS procedure, say P times, is always possible. To assess which of the P returned solutions, say $(\widehat{\mathbf{V}}_1, \widehat{\mathbf{B}}_1), \ldots, (\widehat{\mathbf{V}}_P, \widehat{\mathbf{B}}_P)$, has superior generalized-least-squares fit, we simply feed $(\widehat{\mathbf{V}}_i, \widehat{\mathbf{B}}_i)$ to (33) (using $\widehat{\mathbf{R}}_{\mathrm{y}}$ in place of $\mathbf{R}_{\mathrm{z}}$) and choose

$$\widehat{\mathbf{V}}_{\text{final}}, \widehat{\mathbf{B}}_{\text{final}} = \arg \min_{(\mathbf{V},\mathbf{B}) \in \left\{(\widehat{\mathbf{V}}_1,\widehat{\mathbf{B}}_1),\ldots,(\widehat{\mathbf{V}}_P,\widehat{\mathbf{B}}_P)\right\}} \|\widehat{\mathbf{R}}_{\mathrm{y}}^{-\frac{1}{2}}(\mathbf{Y} - \mathbf{V}\mathbf{B})\|_F^2. \tag{40}$$

The computational complexity of the P-times re-initialized M-IGLS is, of course, $\mathcal{O}(PD(2K^3 + 2LMK + K^2(3L + M) + L^2K))$ where D represents the number of internal iterations in d in Table 1.

10 Experimental Studies on Extraction

A technically firm and keen measure of quality of a hidden-message extraction solution is the difference in bit-error-rate (BER) experienced by the intended recipient and the analyst. The intended recipient in our studies may be using any of the following three message recovery methods: (*i*) Standard carrier matched-filtering (MF) with the known carriers $\mathbf{s}_k$, $k = 1, ..., K$; (*ii*) sample-matrix-inversion MMSE (SMI-MMSE) filtering with known carriers $\mathbf{s}_k$ and estimated host autocorrelation matrix $\widehat{\mathbf{R}}_{\mathrm{y}}$ (see (27)); and (*iii*) ideal MMSE filtering with known carriers $\mathbf{s}_k$ and known true host autocorrelation matrix $\mathbf{R}_{\mathrm{x}}$, which serves as the ultimate performance bound reference for all methods. In terms of blind extraction (neither $\mathbf{s}_k$ nor $\mathbf{R}_{\mathrm{x}}$ known), we will examine: (*iv*) The developed M-IGLS algorithm in Table 1 with $P = 20$ re-initializations and, for comparison purposes, the performance of two typical independent component analysis (ICA) based blind signal separation (BSS) algorithms (v) FastICA [44], and (vi) JADE [45].

We first consider as a host example the gray-scale 512×512 "Baboon" image. We perform 8×8 block DCT embedding by (25) over all bins except the dc coefficient with $K = 4$ distinct arbitrary carriers $\mathbf{s}_k \in \mathbb{R}^{63}$, $k = 1, \ldots, K$. The hidden message embedded by each carrier is $\frac{512^2}{8^2} = 4,096$ bits long. The per-message block mean square distortion due to each embedded message is set to be the same for all messages, i.e. $\mathcal{D}_k = A_k^2 = \frac{\mathcal{D}}{K}$, $k = 1, \ldots, 4$. With per-message $8\times$ 8-block MSE distortion $\mathcal{D}_k$, $k = 1, \ldots, K$, the peak signal-to-noise ratio (PSNR) of the image due to embedding can be calculated by PSNR $\triangleq 20\log_{10}(255) - 10\log_{10}(\sum_{k=1}^{K} \mathcal{D}_k/64)$. Another metric that reflects the relationship between host and embedding distortion is the block document-to-watermark power ratio (DWR) defined as DWR $\triangleq 10\log_{10}\sigma_x^2 - 10\log_{10}(\sum_{k=1}^{K} \mathcal{D}_k)$ where $\sigma_x^2 \triangleq \mathrm{Tr}\{\mathbf{R}_{\mathrm{x}}\}$ is the (total) host block variance. The value of σ_x^2 depends on the nature of each host image and is provided in each experiment that we run (see figure captions) to facilitate translation by the reader between MSE and DWR if desired. For the sake of generality, in our studies we also incorporate white Gaussian noise of variance $\sigma_n^2 = 3$dB.

Fig. 12 shows the average BER (over all $K = 4$ messages) of all methods (i) through (vi) listed above as a function of the host block distortion per-message. FastICA and JADE have computational complexity $\mathcal{O}(2(K-1)(K+M) + 5MK(K+1)/2)$ per iteration and $\mathcal{O}(K(K-1)(4K^2 + 21K + 75)/2)$, respectively. In particular, on an Intel i5-2550K 3.40GHz processor running standard Matlab software for experimentation, the average execution time of the M-IGLS algorithm with $P = 20$ initializations was 1.51 sec, the average execution time of FastICA was 0.20 sec, and the average execution time of JADE was 0.08 sec. While the two independent/principal-component methods (FastICA and JADE) are failing to carry out effective hidden data extraction, to our satisfaction M-IGLS analysis is very close in BER performance to the ideal MMSE detector bound in which both the embedding carriers and the clean host autocorrelation matrix $\mathbf{R}_{\mathrm{x}}$ are treated as perfectly known.

In Fig. 13, we repeat the exact same experimental study on the smaller 256×256 version of the Baboon image in Fig. 11(a) with $K = 4$ hidden messages of length only $\frac{256^2}{8^2} = 1,024$ bits per message (compared to $4,196$ bits per message in Fig. 12). Comparing with Fig. 12, the gap between M-IGLS and ideal MMSE increases as the hidden message size decreases, but the extraction performance of M-IGLS can still be deemed satisfactory. For additional experimental validation, the studies of Fig. 12 and Fig. 13 are repeated on the familiar "Boat" image (shown in Fig. 14) in its 512×512 and 256×256 gray-scale versions (Fig. 15 and Fig. 16, correspondingly).

To examine the behavior of M-IGLS under increasing-density small-message hiding, we consider the 256×256 gray-scale "F-16 Aircraft" image (shown in Fig. 17) with $K = 4$ and $K = 8$ hidden messages of length 1Kbit each. The recovery performance plots for $K = 4$ and $K = 8$ are given in Figs. 18 and 19, correspondingly.

An encompassing conclusion over all executed experiments is that M-IGLS remains a most effective technique to blindly extract hidden messages, while extraction becomes more challenging as the length of the hidden message per used embedding carrier decreases or the number of hidden messages (number of used carriers) increases. It is also worth pointing out that, in these experimental studies, M-IGLS may outperform (in moderate to high distortion values) SMI-MMSE in which the true carriers/signatures are known. This is because SMI-MMSE suffers from performance degradation due to small-sample-support adaptation (estimation of matrix $\mathbf{R}_{\mathrm{y}}$). The unsatisfactory performance of the ICA-based methods is due to the interference from high-amplitude (low-frequency) host coefficients. To demonstrate this point, in Fig. 20 we repeat the exact same experiment of Fig. 12 using this time only the $L = 20$ highest-frequency DCT coefficients as our host vector. It can be observed that, in this moderate host interference environment, ICA-based methods can provide satisfactory performance (not superior to M-IGLS, however). Of course, we may not expect that data are always embedded exclusively in low-amplitude coefficients alone.

Next, for the sake of enhanced experimental credibility, we examine the average performance of the proposed M-IGLS algorithm over a large image database. The experimental image data set, [46] and [47] combined, consists of more than $11,500$ 8-bit gray-scale photographic images which have great variety (e.g., outdoor/indoor, daylight/night, natural/man-made) and different sizes. We embed one up to five messages, $K \in \{1, 2, \dots, 5\}$, via multi-carrier SS embedding with arbitrary carriers and payload between 0.016 and 0.078 bits per pixel (bpp). The length of the embedding carriers varies between 30 and 63, $L \in \{30, 31, \dots, 63\}$. Recovery performance plots are given in Fig. 21. Similar conclusions can be drawn as in the previous individual image host experimentations.

While our blind data extraction algorithmic development was based on the most common SS embedding form (1) for convenience in presentation, the developed algorithm can also be applied to more advanced SS embedding schemes such as improved spread-spectrum (ISS) [13] and correlation-aware improved spread-spectrum (CAISS) [43]. In Fig. 22, we go again over the whole [46], [47] databases under ISS embedding and in Fig. 23 under CAISS embedding (with amplitude-proportion parameter $\eta = 0.7$)[4]. It can be noted from Figs. 22, 23 that M-IGLS analysis can also carry out effective hidden data extraction for the ISS and CAISS schemes.

11 Conclusions on Extraction

We considered the problem of blindly extracting unknown messages hidden in image hosts via multi-carrier/signature spread-spectrum embedding. Neither

[4] Both ISS [13] and CAISS [43] are proposed as single carrier embedding schemes ($K = 1$ in the experiments).

the original host nor the embedding carriers are assumed available. We developed a low complexity multi-carrier iterative generalized least-squares (M-IGLS) core algorithm. Experimental studies showed that M-IGLS can achieve probability of error rather close to what may be attained with known embedding signatures and known original host autocorrelation matrix and presents itself as an effective countermeasure to conventional SS data embedding/hiding[5].

[5] In [39], Bas and Cayre presented an interesting signature-based additive embedding approach different to (25) that is host-vector-by-host-vector dependent and would withstand IGLS-based analysis. The embedding is, however, sensitive to noise which would lead to high recovery error rates by intended recipients and limit the applicability to general covert communication problems.

APPENDIX

A. Derivation of (34)

The minimization in (33) can be carried out in two steps. First, we minimize (33) with respect to $\mathbf{V}$: $\mathbf{V} = \mathbf{Y}\mathbf{B}^T(\mathbf{B}\mathbf{B}^T)^{-1}$ (see also Appendix B). Then, substituting $\mathbf{V}$ back into (33) we obtain

$$\begin{aligned}
\widehat{\mathbf{B}} &= \arg\min_{\mathbf{B}\in\{\pm 1\}^{K\times M}} \|\mathbf{R}_{\mathrm{z}}^{-\frac{1}{2}}(\mathbf{Y} - \mathbf{Y}\mathbf{B}^T(\mathbf{B}\mathbf{B}^T)^{-1}\mathbf{B})\|_F^2 \quad (41)\\
&= \arg\min_{\mathbf{B}\in\{\pm 1\}^{K\times M}} \|\mathbf{R}_{\mathrm{z}}^{-\frac{1}{2}}\mathbf{Y}(\mathbf{I} - \mathbf{B}^T(\mathbf{B}\mathbf{B}^T)^{-1}\mathbf{B})\|_F^2 \quad (42)\\
&= \arg\min_{\mathbf{B}\in\{\pm 1\}^{K\times M}} \|\mathbf{R}_{\mathrm{z}}^{-\frac{1}{2}}\mathbf{Y}\mathbf{P}_{\perp\mathbf{B}}\|_F^2 \quad (43)
\end{aligned}$$

where $\mathbf{P}_{\perp\mathbf{B}} \triangleq \mathbf{I} - \mathbf{B}^T(\mathbf{B}\mathbf{B}^T)^{-1}\mathbf{B}$. ■

B. Proof of (35)

The GLS cost function in (33) can be rewritten as

$$\begin{aligned}
J &\triangleq \|\mathbf{R}_{\mathrm{z}}^{-\frac{1}{2}}\mathbf{Y} - \mathbf{R}_{\mathrm{z}}^{-\frac{1}{2}}\mathbf{V}\mathbf{B}\|_F^2 \quad (44)\\
&= \mathrm{Tr}\left\{\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{Y}\mathbf{Y}^T\right\} - \mathrm{Tr}\left\{\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{Y}\mathbf{B}^T\mathbf{V}^T\right\} - \mathrm{Tr}\left\{\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}\mathbf{B}\mathbf{Y}^T\right\} + \mathrm{Tr}\left\{\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}\mathbf{B}\mathbf{B}^T\mathbf{V}^T\right\} \quad (45)
\end{aligned}$$

where $\mathrm{Tr}\{\cdot\}$ denotes the trace of a matrix.

For a given message matrix $\mathbf{B}$, the GLS optimal estimate of $\mathbf{V}$ can be obtain by differentiating the cost function J with respect to $\mathbf{V}^T$ and setting the outcome equal to the zero matrix,

$$\frac{\partial J}{\partial \mathbf{V}^T} = -\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{Y}\mathbf{B}^T + \mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}(\mathbf{B}\mathbf{B}^T) = \mathbf{0} \Rightarrow \mathbf{V} = \mathbf{Y}\mathbf{B}^T(\mathbf{B}\mathbf{B}^T)^{-1}. \quad (46)$$

■

C. Proof of (36)

We rewrite the GLS cost function in (45) as

$$J = \mathrm{Tr}\left\{\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{Y}\mathbf{Y}^T\right\} - \mathrm{Tr}\left\{\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{Y}\mathbf{B}^T\right\} - \mathrm{Tr}\left\{\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}\mathbf{B}\mathbf{Y}^T\right\} + \mathrm{Tr}\left\{\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}\mathbf{B}\mathbf{B}^T\right\}. \quad (47)$$

Pretend that $\mathbf{V}$ is known and relax the domain of the symbol information matrix to the real space, $\mathbf{B} \in \mathbb{R}^{K\times M}$. The GLS optimal estimate of $\mathbf{B} \in \mathbb{R}^{K\times M}$ can be calculated again by differentiation

$$\frac{\partial J}{\partial \mathbf{B}^T} = -\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{Y} + \mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}\mathbf{B} = \mathbf{0} \Rightarrow \mathbf{B} = (\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V})^{-1}\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{Y}. \quad (48)$$

■

D. Proof of (37)

Since $\mathbf{R}_{\mathrm{y}} = \mathbb{E}\{\mathbf{y}\mathbf{y}^T\} = \mathbf{V}\mathbf{V}^T + \mathbf{R}_{\mathrm{z}}$, by the Matrix Inverse Lemma (also known as Woodbury's matrix identity) [48], we obtain

$$\mathbf{R}_{\mathrm{y}}^{-1} = \mathbf{R}_{\mathrm{z}}^{-1} - \mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}(\mathbf{I} + \mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V})^{-1}\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}. \tag{49}$$

Then,

$$\begin{aligned}
\mathbf{V}^T\mathbf{R}_{\mathrm{y}}^{-1}\mathbf{V} &= \mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V} - \mathbf{V}^T\mathbf{R}_{z}^{-1}\mathbf{V}(\mathbf{I} + \mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V})^{-1}\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V} \\
&= \mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}[\mathbf{I} - (\mathbf{I} + \mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V})^{-1}\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}] \\
&= \mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}(\mathbf{I} + \mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V})^{-1}[(\mathbf{I} + \mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}) - \mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}] \\
&= \mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}(\mathbf{I} + \mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V})^{-1}. \qquad (50)
\end{aligned}$$

By the property of the inverse of a product of matrices [48], the inverse of $(\mathbf{V}^T\mathbf{R}_{\mathrm{y}}^{-1}\mathbf{V})$ is

$$\begin{aligned}
(\mathbf{V}^T\mathbf{R}_{\mathrm{y}}^{-1}\mathbf{V})^{-1} &= (\mathbf{I} + \mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V})(\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V})^{-1} \\
&= (\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V})^{-1} + \mathbf{I}. \qquad (51)
\end{aligned}$$

We combine the results of (49) and (51) and finally obtain

$$\begin{aligned}
(\mathbf{V}^T\mathbf{R}_{\mathrm{y}}^{-1}\mathbf{V})^{-1}\mathbf{V}^T\mathbf{R}_{\mathrm{y}}^{-1} &= \left((\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V})^{-1} + \mathbf{I}\right)\mathbf{V}^T\left(\mathbf{R}_{\mathrm{z}}^{-1} - \mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V}(\mathbf{I} + \mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V})^{-1}\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\right) \\
&= (\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}\mathbf{V})^{-1}\mathbf{V}^T\mathbf{R}_{\mathrm{z}}^{-1}. \qquad (52)
\end{aligned}$$

■

References

[1] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding: A survey," *Proc. IEEE (Special Issue on Identification and Protection of Multimedia Information)*, vol. 87, pp. 1062-1078, July 1999.

[2] I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking.* San Francisco, CA: Morgan-Kaufmann, 2002.

[3] F. Hartung and M. Kutter, "Multimedia watermarking techniques," *Proc. IEEE (Special Issue on Identification and Protection of Multimedia Information)*, vol. 87, pp. 1079-1107, July 1999.

[4] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking digital image and video data: A state-of-the-art overview," *IEEE Signal Processing Magazine*, vol. 17, pp. 20-46, Sept. 2000.

[5] N. F. Johnson and S. Katzenbeisser, "A survey of steganographic techniques," in *Information Hiding*, S. Katzenbeisser and F. Petitcolas Eds. Norwood, MA: Artech House, 2000, pp. 43-78.

[6] S. Wang and H. Wang, "Cyber warfare: Steganography vs. steganalysis," *Communications of the ACM*, vol. 47, pp. 76-82, Oct. 2004.

[7] C. Cachin, "An information-theoretic model for steganography," in *Proc. 2nd Intern. Workshop on Information Hiding*, Portland, OR, Apr. 1998, pp. 306-318.

[8] G. J. Simmons, "The prisoner's problem and the subliminal channel," in *Advances in Cryptology: Proc. CRYPTO'83.* New York, NY: Plenum, 1984, pp. 51-67.

[9] J. Fridrich, *Steganography in Digital Media, Principles, Algorithms, and Applications.* Combridge, UK: Combridge Univeristy Press, 2010.

[10] Y. Wang and P. Moulin, "Perfectly secure steganography: Capacity, error exponents, and code constructions," *IEEE Trans. Inform. Theory*, vol. 54, pp. 2706-2722, June 2008.

[11] *Federal plan for cyber security and information assurance research and development*, Interagency Working Group on Cyber Security and Information Assurance, Apr. 2006.

[12] R. Chandramouli, "A mathematical framework for active steganalysis," *ACM Multimedia Systems Special Issue on Multimedia Watermarking*, vol. 9, pp. 303-311, Sept. 2003.

[13] H. S. Malvar and D. A. Florencio, "Improved spread spectrum: A new modulation technique for robust watermarking," *IEEE Trans. Signal Proc.*, vol. 51, pp. 898-905, Apr. 2003.

[14] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shannon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Proc.*, vol. 6, pp. 1673-1687, Dec. 1997.

[15] J. Hernandez, M. Amado, and F. Perez-Gonzalez, "DCT-domain watermarking techniques for still images: Detector performance analysis and a new structure," *IEEE Trans. Image Proc.*, vol. 9, pp. 55-68, Jan. 2000.

[16] C. Qiang and T. S. Huang, "An additive approach to transform-domain information hiding and optimum detection structure," *IEEE Trans. Multimedia*, vol. 3, pp. 273-284, Sept. 2001.

[17] C. Fei, D. Kundur, and R. H. Kwong, "Analysis and design of watermarking algorithms for improved resistance to compression," *IEEE Trans. Image Proc.*, vol. 13, pp. 126-144, Feb. 2004.

[18] M. Gkizeli, D. A. Pados, and M. J. Medley, "SINR, bit error rate, and Shannon capacity optimized spread-spectrum steganography," in *Proc. IEEE Intern. Conf. Image Proce. (ICIP)*, Singapore, Oct. 2004, pp. 1561-1564.

[19] M. Gkizeli, D. A. Pados, S. N. Batalama, and M. J. Medley, "Blind iterative recovery of spread-spectrum steganographic messages," in *Proc. IEEE Intern. Conf. Image Proc. (ICIP)*, Genova, Italy, Sept. 2005, vol. 2, pp. 11-14.

[20] M. Gkizeli, D. A. Pados, and M. J. Medley, "Optimal signature design for spread-spectrum steganography," *IEEE Trans. Image Proc.*, vol. 16, pp. 391-405, Feb. 2007.

[21] F. Cayre, C. Fontaine, and T. Furon, "Watermarking security: Theory and practice," *IEEE Trans. Signal Proc.*, vol. 53, pp. 3976-3987, Oct. 2005.

[22] L. Pérez-Freire, P. Comesana, J. R. Troncoso-Pastoriza, and F. Pérez-González, "Watermarking security: A survey," *LNCS Transactions on Data Hiding and Multimedia Security*, 2006.

[23] M. Barni, F. Bartolini, and T. Furon, "A general framework for robust watermarking security," *ACM Journal Signal Proc. - Special Section: Security of Data Hiding Technologies*, vol. 83, pp. 2069-2084, Oct. 2003.

[24] L. Pérez-Freire and F. Pérez-González, "Spread-spectrum watermarking security," *IEEE Trans. Inform. Forensics and Security*, vol. 4, pp. 2-24, Mar. 2009.

[25] S. Lyu and H. Farid, "Steganalysis using higher-order image statistics," *IEEE Trans. Inform. Forensics and Security*, vol. 1, pp. 111-119, Mar. 2006.

[26] K. Sullivan, U. Madhow, S. Chandrasekaran, and B. S. Manjunath, "Steganalysis for Markov cover data with applications to images," *IEEE Trans. Inform. Forensics and Security*, vol. 1, pp. 275-287, June 2006.

[27] İ. Avcıbaş, N. Memon, and B. Sankur, "Steganalysis using image quality metrics," *IEEE Trans. Image Proc.*, vol. 12, pp. 221-229, Feb. 2003.

[28] W. Lie and G. Lin, "A feature-based classification technique for blind image steganalysis," *IEEE Trans. Multimedia*, vol. 7, pp. 1007-1020, Dec. 2005.

[29] G. Gul and F. Kurugollu, "SVD-based universal spatial domain image steganalysis," *IEEE Trans. Inform. Forensics and Security*, vol. 5, pp. 349-353, June 2010.

[30] Y. Wang and P. Moulin, "Steganalysis of block-DCT image steganography," in *Proc. IEEE Workshop on Statistical Signal Processing*, Saint-Louis, MO, Sept. 2003, pp. 339-342.

[31] Y. Wang and P. Moulin, " Optimized feature extraction for learning-based image steganalysis," *IEEE Trans. Inform. Forensics and Security*, vol. 2, pp. 31-45, Mar. 2007.

[32] B. Li, J. Huang, and Y. Q. Shi, "Steganalysis of YASS," *IEEE Trans. Inform. Forensics and Security*, vol. 4, pp. 369-382, Sept. 2009.

[33] M. Li, D. A. Pados, S. N. Batalama, and M. J. Medley, "Passive spread-spectrum steganalysis," in *Proc. IEEE Intern. Conf. Image Proc. (ICIP)*, Brussels, Belgium, Sept. 2011, pp. 1997-2000.

[34] D. G. Manolakis, V. K. Ingle, and S. M. Kogon. *Statistical and adaptive signal processing: Spectral estimation, signal modeling, adaptive filtering and array processing.* Boston, MA: McGraw-Hill, 2000.

[35] J. M. M. Anderson, B. A. Mair, M. Rao, and C.-H. Wu, "Weighted least-squares reconstruction methods for positron emission tomography," *IEEE Trans. Medical Imaging*, vol. 16, pp. 159-165, Apr. 1997.

[36] J. Eriksson and M. Viberg, "Asymptotic properties of nonlinear weighted least squares in radar array processing," *IEEE Trans. Signal Proc.*, vol. 52, pp. 3083-3095, Nov. 2004.

[37] S. Talwar, M. Viberg, and A. Paulraj, "Blind seperation of synchronous co-channel digital signals using an antenna array - Part I: Algorithms," *IEEE Trans. Signal Proc.*, vol. 44, pp. 1184-1197, May 1996.

[38] T. Li and N. D. Sidiropoulos, "Blind digital signal separation using successive interference cancellation iterative least squares," *IEEE Trans. Signal Proc.*, vol. 48, pp. 3146-3152, Nov. 2000.

[39] P. Bas and F. Cayre, "Achieving subspace or key security for WOA using natural or circular watermarking," in *Proc. ACM Multimedia and Security Workshop*, Geneva, Switzerland, Sept. 2006.

[40] T. M. Cover and J. A. Thomas. *Elements of Information Theory*, 2nd ed. Hoboken, NJ: John Wiley, 2006.

[41] M. Li, S. N. Batalama, and D. A. Pados, "Population size identification for CDMA eavesdropping," in *Proc. IEEE Military Comm. Conf. (MILCOM)*, Orlando, FL, Oct. 2007, pp. 1-6.

[42] G. N. Karystinos and D. A. Pados, "Supervised phase correction of blind space-time DS/CDMA channel estimates," *IEEE Trans. Commun.*, vol. 55, pp. 584-592, Mar. 2007.

[43] A. Valizadeh and Z. J. Wang, "Correlation-and-bit-aware spread spectrum embedding for data hiding," *IEEE Trans. Inform. Forensics and Security*, vol. 6 , pp. 267-282, June 2011.

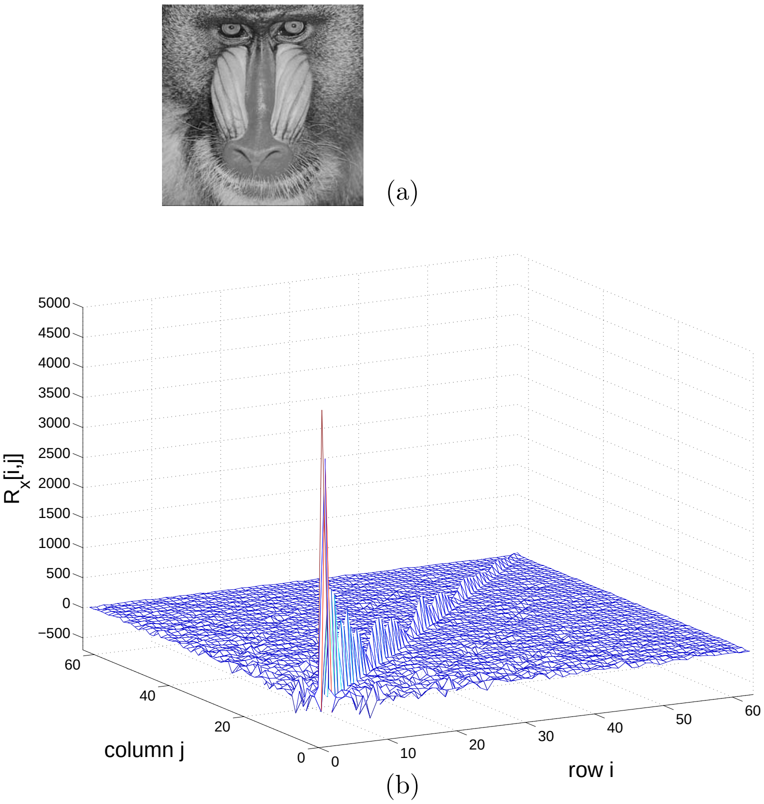
[44] A. Hyvärinen and E. Oja, "A fast fixed-point algorithm for independent component analysis," *Neural Computation*, vol. 9, pp. 1483-1492, Oct. 1997.

[45] J. F. Cardoso, "High-order contrasts for independent component analysis," *Neural Computation*, vol. 11, pp. 157-192, Jan. 1999.

[46] T. Filler, T. Pevny, and P. Bas. *BOSS, Break Our Steganography System.* Available: http: //www.agents.cz/boss/

[47] G. Schaefer and M. Stich, “UCID–An uncompressed colour image database,” in *Proc. SPIE, Storage and Retrieval Methods and Applications for Multimedia*, San Jose, CA, Jan. 2004, pp. 472-480.

[48] C. D. Meyer. *Matrix Analysis and Applied Linear Algebra*, Philadelphia, PA: SIAM, 2000



(a)

(b)

Figure 11: (a) Baboon image example $\mathbf{H} \in \{0, 1, ..., 255\}^{256\times256}$. (b) Host data autocorrelation matrix (8 × 8 DCT, 63-bin host) [20].

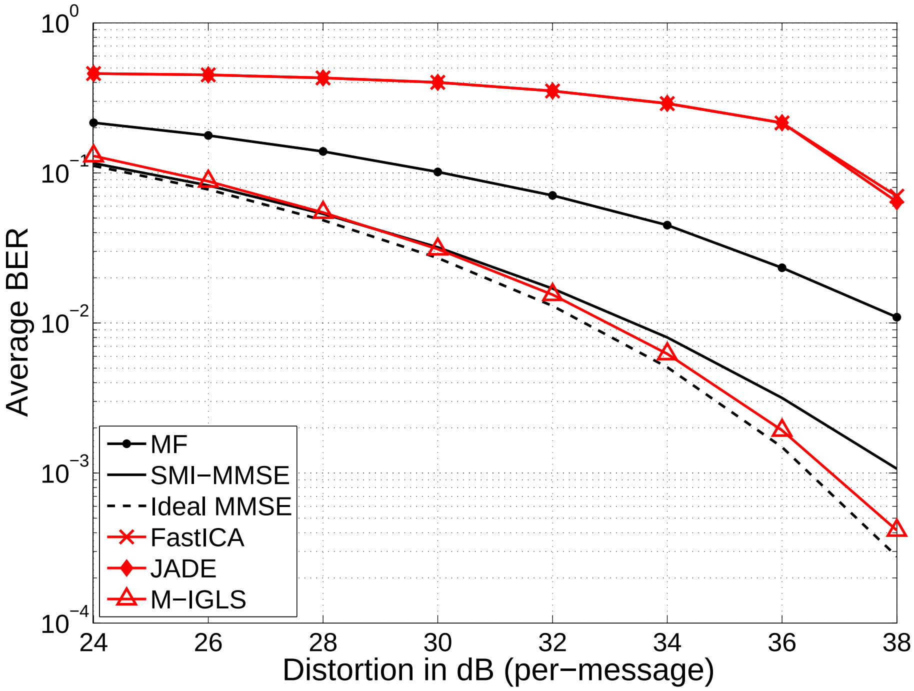


Figure 12: Average BER versus per-message block distortion (512×512 Baboon, $L = 63$, $K = 4$ messages of 4Kbits each, $\sigma_n^2 = 3$dB, $\sigma_x^2 = 46.49$dB).

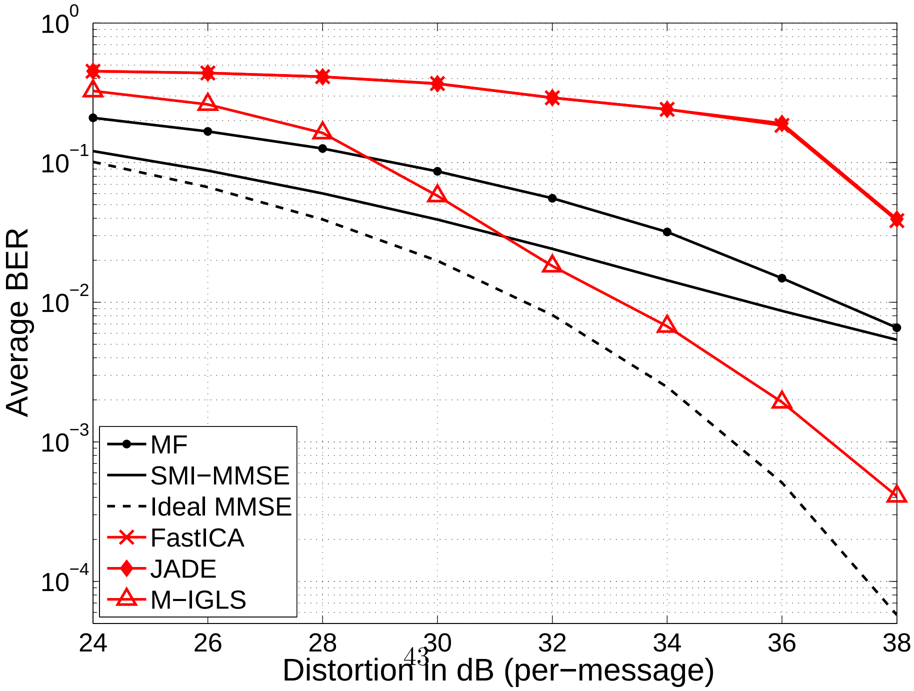


Figure 13: Average BER versus per-message block distortion (256×256 Baboon, $L = 63$, $K = 4$ messages of 1Kbit each, $\sigma_n^2 = 3$dB, $\sigma_x^2 = 45.45$dB).

Figure 14: 512 × 512 gray-scale Boat image.

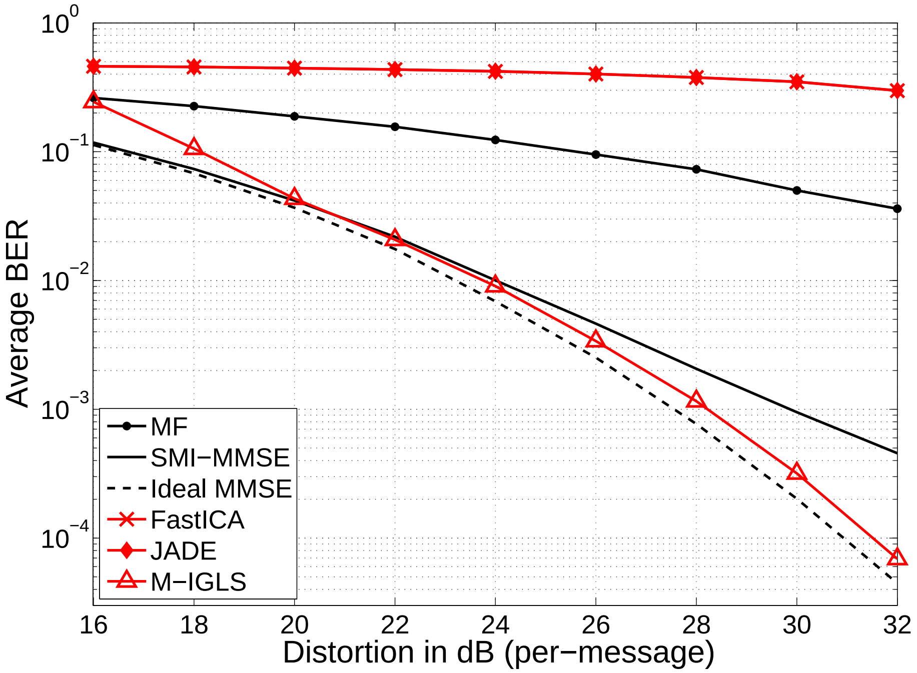


Figure 15: Average BER versus per-message block distortion (512 × 512 Boat, $L = 63$, $K = 4$ messages of 4Kbits each, $\sigma_n^2 = 3$dB, $\sigma_x^2 = 44.15$dB).

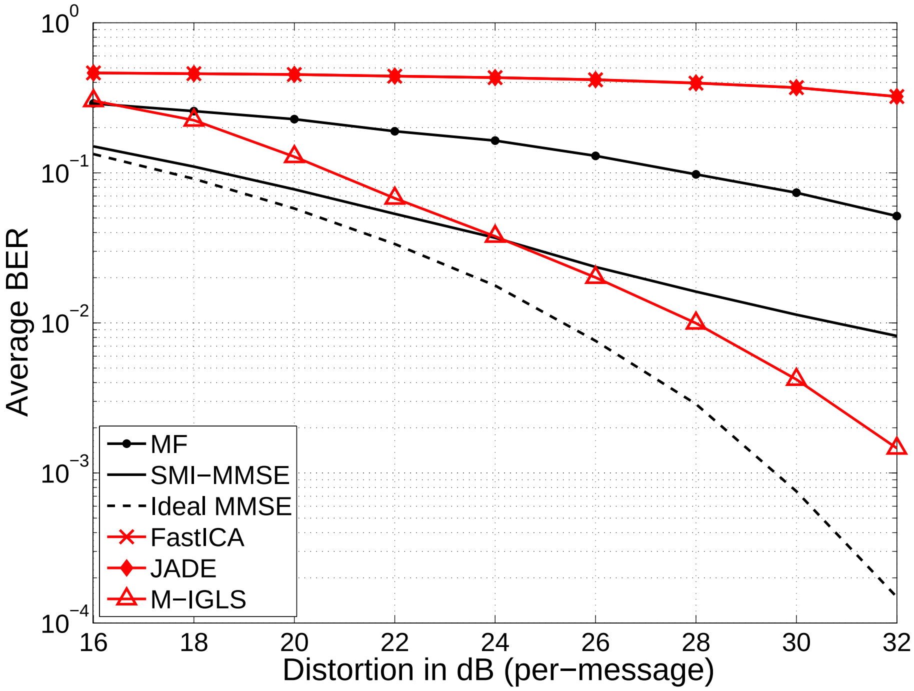


Figure 16: Average BER versus per-message block distortion, 256 × 256 Boat, $L = 63$, $K = 4$ messages of 1Kbit each, $\sigma_n^2 = 3$dB, $\sigma_x^2 = 45.57$dB).

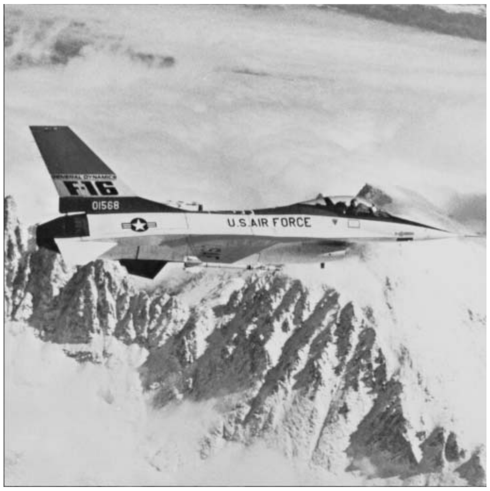


Figure 17: 256 × 256 gray-scale Aircraft image.

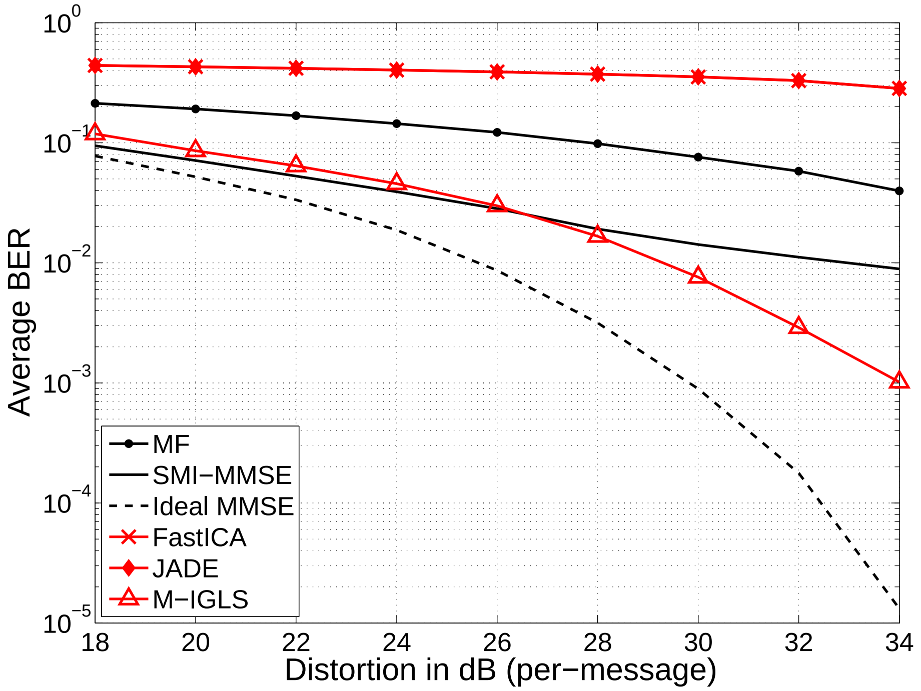


Figure 18: Average BER versus per-message block distortion (256 × 256 F16 Aircraft, $L = 63$, $K = 4$ messages of 1Kbit each, $\sigma_n^2 = 3$dB, $\sigma_x^2 = 46.23$dB).

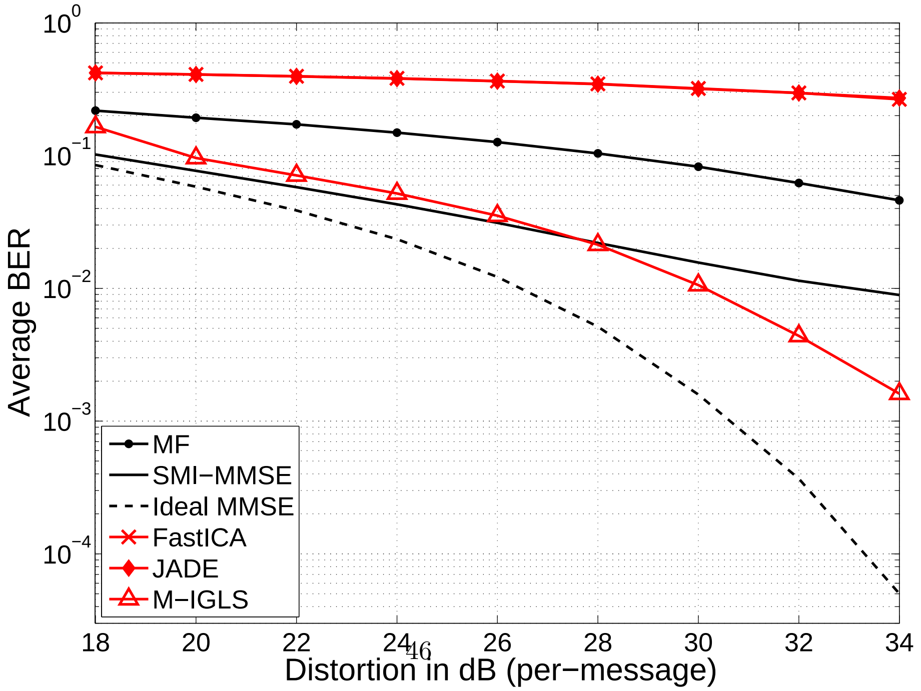


Figure 19: Average BER versus per-message block distortion (256 × 256 F16 Aircraft, $L = 63$, $K = 8$ messages of 1Kbit each, $\sigma_n^2 = 3$dB, $\sigma_x^2 = 46.23$dB).

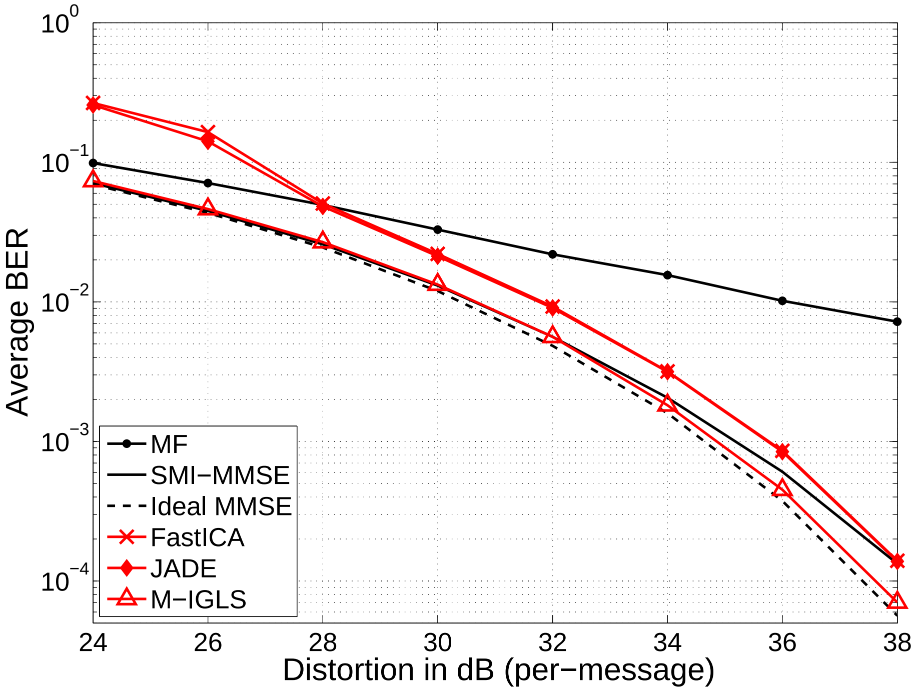


Figure 20: Average BER versus per-message block distortion (512×512 Baboon, $L = 20$ highest-frequency coefficients, $K = 4$ messages of 4Kbits each, $\sigma_n^2 = 3$dB, $\sigma_x^2 = 46.49$dB).

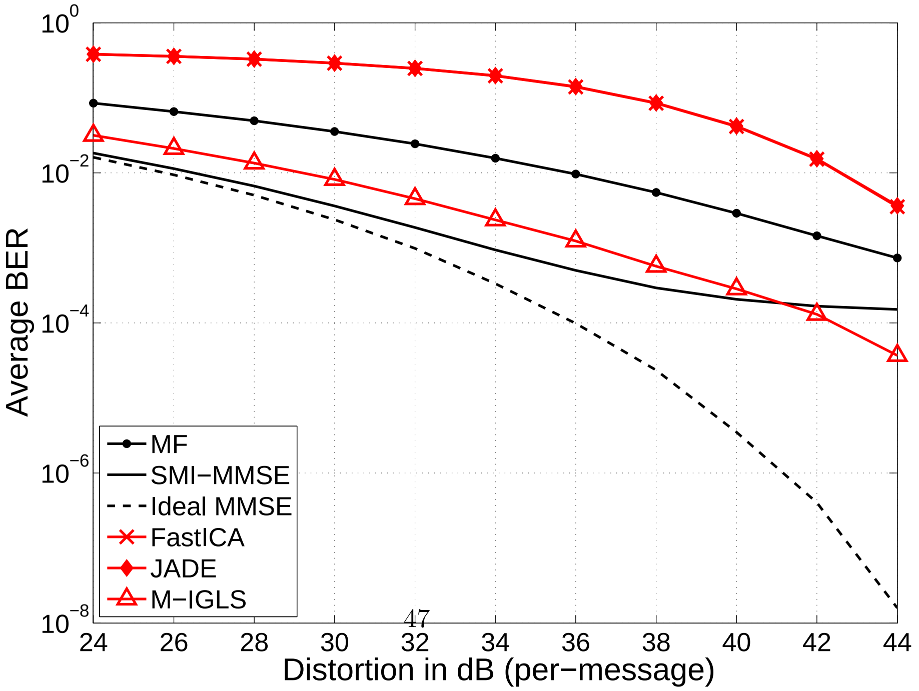


Figure 21: Average BER versus per-message block distortion (average findings over a dataset of more than $11,500$ images [46], [47], $K = 1$, $L \in \{30, 31, \ldots, 63\}$, $\sigma_n^2 = 3$dB, average $\sigma_x^2 = 41.63$dB).

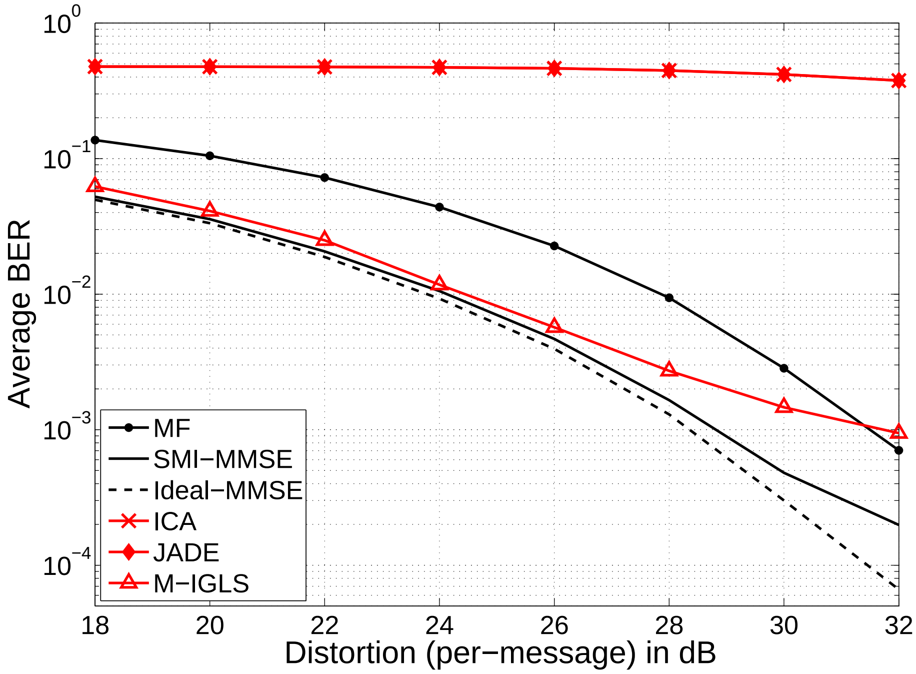


Figure 22: Average BER versus per-message block distortion (average findings over a dataset of more than $11,500$ images [46], [47], ISS embedding [13], $K = 1$, $L \in \{30, 31, \ldots, 63\}$, $\sigma_n^2 = 3$dB, average $\sigma_x^2 = 41.63$).

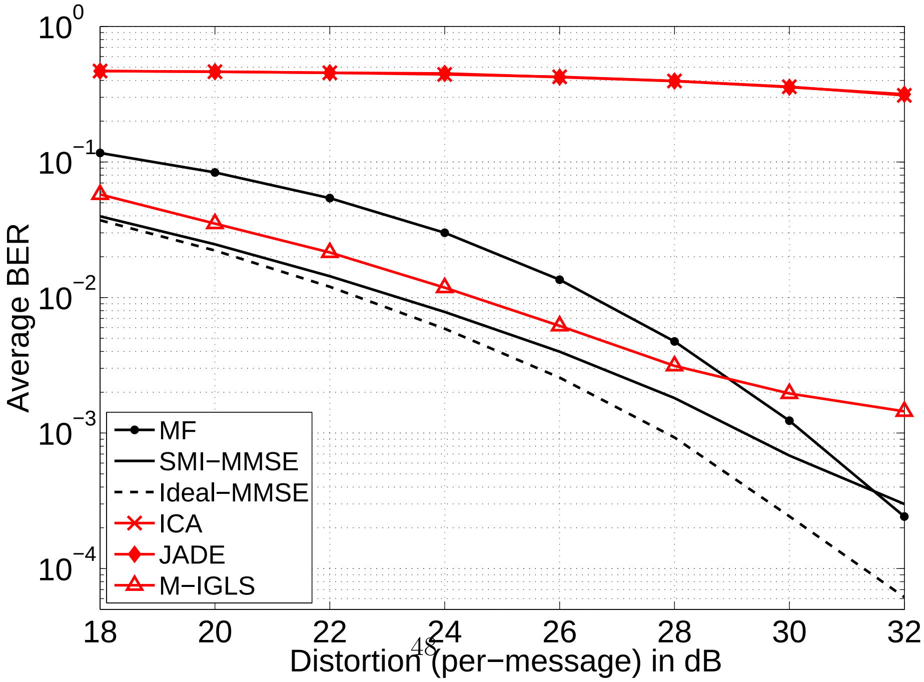


Figure 23: Average BER versus per-message block distortion (average findings over a dataset of more than $11,500$ images [46], [47], CAISS embedding [43], ($\eta = 0.7$), $K = 1$, $L \in \{30, 31, \ldots, 63\}$, $\sigma_n^2 = 3$dB, average $\sigma_x^2 = 41.63$dB).

1.

1. Report Type

Final Report

Primary Contact E-mail
Contact email if there is a problem with the report.

pados@buffalo.edu

Primary Contact Phone Number
Contact phone number if there is a problem with the report

716-645-1150

Organization / Institution name

State University of New York at Buffalo

Grant/Contract Title
The full title of the funded effort.

Insertion, Detection, and Extraction of Messages Hidden by Optimal Multi-signature Spread-Spectrum Means

Grant/Contract Number
AFOSR assigned control number. It must begin with "FA9550" or "F49620" or "FA2386".

FA9550-12-1-0123

Principal Investigator Name
The full name of the principal investigator on the grant or contract.

Dimitris A Pados

Program Manager
The AFOSR Program Manager currently assigned to the award

Dr. Tristan Nguyen

Reporting Period Start Date

04/01/2012

Reporting Period End Date

03/31/2015

Abstract

We carry out optimized spread-spectrum data embedding in a given digital image (or audio, or video sequence). First, the overall image/host medium is pre-processed into transform-domain small blocks from which host vectors are obtained via zig-zag scanning vectorization. Multiuser data embedding is performed in the generated host vectors. Under this data embedding model, we calculate an orthogonal set of embedding spread-spectrum signatures that achieves maximum sum signal-to-interference-plus-noise ratio (sum-SINR) at the output of the linear-filter receivers for any fixed embedding amplitude values. Then, for any given total embedding distortion constraint, we present the optimal multi-signature assignment and amplitude allocation that maximizes the sum capacity of the embedding procedure. The practical implication of the reported results is sum-SINR, sum-capacity optimal multiuser/multi-signature spread-spectrum data embedding in the digital medium. Extensive experiments that we carried out demonstrate the effectiveness of the proposed methods. The problem of extracting blindly data embedded over a wide band in a spectrum (transform) domain of a digital medium is also considered.

Distribution Statement
This is block 12 on the SF298 form.

Distribution A - Approved for Public Release

Explanation for Distribution Statement

If this is not approved for public release, please provide a short explanation. E.g., contains proprietary information.

SF298 Form

Please attach your SF298 form. A blank SF298 can be found here. Please do not password protect or secure the PDF The maximum file size for an SF298 is 50MB.

AFD-070820-035.pdf

Upload the Report Document. File must be a PDF. Please do not password protect or secure the PDF . The maximum file size for the Report Document is 50MB.

FINAL_REPORT.pdf

Upload a Report Document, if any. The maximum file size for the Report Document is 50MB.

Archival Publications (published) during reporting period:

[1] L. Wei, D. A. Pados, S. N. Batalama, Rose Q. Hu, and M. J. Medley, ‘‘Optimal multiuser spread-spectrum data hiding in digital images,’’ Security Comm. Networks (Wiley), DOI: 10.1002/sec.1001, pp. 1-10, Nov. 2014.

[2] M. Li, M. Kulhandjian, D. A. Pados, S. N. Batalama, and M. J. Medley, ‘‘Extracting spread-spectrum hidden data from digital media,’’ IEEE Transactions on Information Forensics and Security, vol. 8, pp. 1201-1210, July 2013 (4.6K DOWNLOADS FROM ResearchGate.)

[3] L. Wei and D. A. Pados, ‘‘Optimal orthogonal carriers and sum-SINR/sum-capacity of the multiple-access vector channel,’’ IEEE Transactions on Communications, vol. 60, pp. 1188-1192, May 2012.

[4] Lili Wei, D. A. Pados, S. N. Batalama, M. J. Medley, and Rose Q. Hu, ‘‘Advances in multiuser data embedding in digital media: Orthogonal sum-SINR-optimal carriers,” in Proceedings IEEE ICC 2014 (International Conf. on Comm.), Comm. and Inform. Syst. Security Symposium, Sydney, Australia, June 10-14, 2014, pp. 969-974.

[5] Ming Li, N. Thawdar, D. A. Pados, S. N. Batalama, and M. J. Medley, “Minimum-distortion data embedding in video streams,” in Proceedings IEEE ICC 2014 (International Conf. on Comm.), Signal Proc. for Comm. Symposium, Sydney, Australia, June 10-14, 2014, pp. 4600-4605.

[6] M. Li, M. Kulhandjian, D. A. Pados, S. N. Batalama, M. J. Medley, and J. D. Matyjas, ‘‘On the extraction of spread-spectrum hidden data in digital media,” in Proceedings IEEE ICC 2012 (International Conf. on Comm.), Comm. and Inform. Syst. Security Symposium, Ottawa, Canada, June 10-15, 2012, pp. 1031-1035.

[7] L. Wei, Rose Q. Hu, Geng Wu, and D. A. Pados, “Optimal multiuser spread-spectrum data embedding in videos streams,” in Proceedings IEEE GLOBECOM 2014, Comm. and Inform. Syst. Security Symposium, Austin, TX, Dec. 8-12, 2014, pp. 764-769 (BEST of GLOBECOM 2014 - TOP 50 PAPERS SPECIAL PRESENTATION).

See also:
[8] Lili Wei, Geng Wu, and Rose Hu, ``Sum-Capacity Optimal Spread-Spectrum Data Hiding in Video Streams,” in Proceedings IEEE ICC 2015, London, UK, June 2015,
pp. 9035-9040 (THE 2015 IEEE International Conference on Communications BEST PAPER AWARD IN COMMUNICATION AND INFORMATION SYSTEM SECURITY).

Changes in research objectives (if any):

N/A

Change in AFOSR Program Manager, if any:

New AFOSR Program Manager:
Dr. Tristan Nguyen (703) 696-7796
DSN 426-7796 FAX (703) 696-7360
Email: Info.Security@afosr.af.mil

Extensions granted or milestones slipped, if any:

N/A

AFOSR LRIR Number

LRIR Title

Reporting Period

Laboratory Task Manager

Program Officer

Research Objectives

Technical Summary

Funding Summary by Cost Category (by FY, $K)

	Starting FY	FY+1	FY+2
Salary			
Equipment/Facilities			
Supplies			
Total			

Report Document

Report Document - Text Analysis

Report Document - Text Analysis

Appendix Documents

2. Thank You

E-mail user

Jun 30, 2015 15:07:18 Success: Email Sent to: pados@buffalo.edu